HP BladeSystem Onboard Administrator Benutzerhandbuch

Übersicht

Dieses Handbuch enthält Informationen zur erstmaligen Einrichtung und Inbetriebnahme des HP Blade System Onboard Administrator. Es geht auch auf die Verwendung der Onboard Administrator-GUI und des Insight Display des Gehäuses ein. Die Informationen in diesem Handbuch gelten für Version 4.40 (oder höher) des HP Blade System Onboard Administrator.

© Copyright 2006, 2015 Hewlett-Packard Development Company, L.P.

Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Garantien für HP Produkte und Services werden ausschließlich in der entsprechenden, zum Produkt bzw. zum Service gehörenden Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. Hewlett-Packard („HP“) haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Teilenummer: 695522-048

März 2015

Ausgabe: 23

Vertrauliche Computersoftware. Für Besitz, Nutzung und Kopieren ist eine gültige Lizenz von HP erforderlich. In Übereinstimmung mit FAR 12.211 und 12.212 sind kommerzielle Computersoftware, Computersoftware-Dokumentation und technische Daten für kommerzielle Komponenten für die US-Regierung mit der Standardlizenz des Herstellers lizenziert.

Microsoft®, Windows®, Windows Vista®, Windows® XP, Windows® 7 und Windows Server® sind in den USA eingetragene Marken der Microsoft Unternehmensgruppe. Google™ ist eine Marke von Google Inc. Java ist eine eingetragene Marke der Oracle Corporation und/oder ihrer Tochtergesellschaften. Red Hat® ist in den USA und anderen Ländern eine eingetragene Marke von Red Hat, Inc. UNIX® ist eine eingetragene Marke von The Open Group.

Inhaltsverzeichnis

1 Einführung 1

Übersicht 1

Zugriffsanforderungen 3

Übersicht über Onboard Administrator 4

Schnittstellen 6

Onboard Administrator-Authentifizierung 7

Erstmaliges Ausführen von Onboard Administrator 8

Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator 10

Flash-Notfallwiederherstellung 12

Ausführen des Konfigurationsassistenten 13

Verwenden der Online-Hilfe 14

Ändern von Gehäuse- und Komponentenkonfigurationen 14

Wiederherstellen des Administratorkennworts 15

Sicherheitshinweise 16

Übersicht über die BladeSystem-Netzwerkarchitektur 16

Empfohlene optimale Vorgehensweisen bezüglich Sicherheit 16

Netzwerkports 18

Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18

2 HP BladeSystem c3000/c7000-Gehäuse – Hardwareinstallation 25

Installieren von Onboard Administrator-Modulen 25

HP BladeSystem Onboard Administrator-Verkabelung 25

3 HP BladeSystem Insight Display 28

HP BladeSystem c7000 2-Zoll Insight Display-Komponenten 28

HP BladeSystem c3000 und c7000 3-Zoll Insight Display-Komponenten 29

Insight Display – Übersicht 29

Zugreifen auf das HP BladeSystem c3000 Insight Display 30

Durchführen der Insight Display-Installation 31

Navigieren im Insight Display 37

Bildschirm „Health Summary“ (Zustand – Zusammenfassung) 39

Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) 40

Bildschirm „Enclosure Info“ (Gehäuse-Info) 41

Bildschirm „Blade or Port Info“ (Blade- oder Port-Info) 41

Bildschirm „Turn Enclosure UID On/Off“ (Gehäuse-UID aktivieren/deaktivieren) 43

Bildschirm „View User Note“ (Benutzernotiz anzeigen) 44

Bildschirm „Chat Mode“ (Chat-Modus) 44
Bildschirm „USB Menu“ (USB-Menü) 45
Bildschirm „KVM Menu“ (KVM-Menü) 46
Insight Display-Fehlermeldungen 47
Stromversorgungsfehler 47
Kühlungsfehler 47
Positionsfehler 48
Konfigurationsfehler 48
Komponentenausfallfehler 48

4 Gehäuse-KVM 50
Funktionen 50

5 Assistent für die Erstkonfiguration (First Time Setup Wizard) 55
Bevor Sie beginnen 55
Anmelden bei Onboard Administrator 55
Benutzereinstellungen 56
FIPS 57
Bildschirm „Enclosure Selection“ (Gehäuseauswahl) 59
Bildschirm „Configuration Management“ (Konfigurationsverwaltung) 60
Bildschirm „Rack and Enclosure Settings“ (Rack- und Gehäuseeinstellungen) 61
Bildschirm „Administrator Account Setup“ (Einrichten des Administratorkontos) 64
Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub) 66
Bildschirm „Directory Groups Configuration“ (Konfiguration von Verzeichnisgruppen) 74
Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 76
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Bildschirm „Enclosure SNMP Settings“ (SNMP-Gehäuseeinstellungen) 86
Bildschirm „Power Management“ (Stromversorgungsverwaltung) 88
Finish (Fertig stellen) 93

6 Navigieren in Onboard Administrator 94
Navigationsübersicht 94
Strukturansicht 94
Navigation in der grafischen Ansicht 97

7 Ansicht des Racks 100
Bildschirm „Rack Overview“ (Rack-Übersicht) 100
Topologie-Modi 102

Registerkarte „Rack Topology“ (Rack-Topologie) 103
Registerkarte „Power and Thermal“ (Stromversorgung und Wärmewerte) 105
Bildschirm „Rack Firmware“ (Rack-Firmware) 106

8 Konfigurieren von HP BladeSystem-Gehäusen und Gehäusekomponenten 110
Anzeigen der Statusbildschirme 110
Gehäuseeinstellungen 111
Auswählen von Gehäusen 111
Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
AlertMail 116
Registerkarten „Device Power Sequence Device Bays“ (Komponenten-Startsequenz der Geräteeinschübe) 120
Registerkarte „Device Power Sequence Interconnect Bays“ (Komponenten-Startsequenz der Verbindungsmoduleinschübe) 123
Datum und Uhrzeit 123
Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
Registerkarte „IPv4-Einstellungen“ 126
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
Registerkarte „NIC Options“ (NIC-Optionen) 135
Registerkarte „Advanced Settings“ (Erweiterte Einstellungen) 135
Network Access (Netzwerkzugriff) 136
Registerkarte „Trusted Hosts“ (Vertrauenswürdige Hosts) 138
Registerkarte „Anonymous Data“ (Anonyme Daten) 139
Registerkarte „FIPS“ 140
Registerkarte „Login Banner“ (Anmelde-Banner) 142
Link Loss Failover (Failover bei Verbindungsverlust) 143
SNMP-Einstellungen 143
Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub) 148
EBIPA für IPv4 151
EBIPA für IPv6 154
Device Summary (Komponentenzusammenfassung) 158
Active to Standby (Aktiv in Standby) 161
DVD-Laufwerk 162
Interaktive Installation und Konfiguration des DVD/CD-ROM-Laufwerks 164
Unbeaufsichtigte Bereitstellung des Betriebssystems 170
Sofortzugriff auf DVD-basierte Medien zur Installation von Anwendungen und für den Datenimport 176
Aktualisieren der Blade-Firmware mit HP Smart Update Manager 176
VLAN-Konfiguration 177
VLAN-Einstellungen 178
Hinzufügen, Bearbeiten und Entfernen von VLANs 180

Konfigurieren von Geräten ... 182
Active Health System ... 184
Insight Remote Support-Registrierung ... 184
Insight Remote Support-Serviceereignisse ... 192
Insight Remote Support-Datensammlungen ... 193
Datensammlungsinformationen ... 194
Remote Support-Zertifikatverwaltung ... 194
Remote Support-Registerkarte „Certificate Upload“ (Zertifikat-Upload) ... 196
Enclosure Firmware Management ... 197
Manuelle Ermittlung ... 204
Manuelle Aktualisierung ... 205
Enclosure Firmware Management-Protokoll ... 205
Statusaktualisierungen ... 206
Verwalten von Gehäusen ... 207
Ausschalten des Gehäuses ... 207
Verbinden von Gehäusen ... 207
Verwalten von mehreren Gehäusen ... 208
Aktives Onboard Administrator-Modul ... 208
Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator) ... 208
Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des aktiven Onboard Administrator-Moduls ... 210
USB-Registerkarte des aktiven Onboard Administrator-Moduls ... 211
Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator ... 212
Registerkarte „Certificate Administration Information“ (Zertifikatsverwaltungsinformationen) ... 216
Registerkarte „Certificate Request“ (Zertifikat-Anforderung) ... 218
Registerkarte „Certificate Upload“ (Zertifikat-Upload) ... 221
Firmware-Aktualisierung ... 222
Registerkarte „Language Pack“ (Sprachpaket) ... 225
Systemprotokoll ... 226
Registerkarte „Log Options“ (Protokolloptionen) ... 227
Onboard Administrator Standby-Modul ... 228
Bildschirm „Standby Onboard Administrator“ ... 228
Registerkarte „Virtual Buttons“ des Onboard Administrator-Standby-Moduls ... 229
Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA ... 230
Registerkarte „Information“ (Informationen) auf dem Bildschirm „Standby Onboard Administrator Certificate Administration“ (Zertifikatverwaltung des Onboard Administrator-Standby-Moduls) ... 232
Registerkarte „Certificate Request“ (Zertifikat-Anforderung) des Standby-Moduls ... 234
Registerkarte „Certificate Upload“ (Zertifikat-Upload) des Standby-Moduls ... 236

Systemprotokoll für Standby-Onboard Administrator 236
Standby to Active (Standby in Aktiv) 237
Geräteeinschübe 237
Geräteeinschübe 237
Registerkarte „Device Bay Status“ (Status des Geräteeinschubs) 240
Registerkarte „Server Blade Information“ (Server Blade-Informationen) 245
Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade) 248
Registerkarte „Boot Options“ (Startoptionen) 250
Registerkarte „IML Log“ 252
iLO-Bildschirm 253
Registerkarte „iLO Event Log“ (iLO-Ereignisprotokoll) 255
Portzuordnung 255
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 257
Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 259
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse 263
Tabellenansicht der Portzuordnungen der Geräteeinschübe für das c7000-Gehäuse 266
Firmware 270
Starten einer manuellen Aktualisierung oder Ermittlung 272
Einzelne Server 272
Mehrere Server 273
Firmware-Management-Protokolle 275
Anzeigen der Firmware-Versionen 277
Abweichende Firmwareversionen 279
Speicher-Blades 279
Informationen zum I/O-Erweiterungs-Blade 284
Registerkarte mit den virtuellen Geräten des I/O-Erweiterungs-Blade 285
Registerkarte mit Informationen zum I/O-Erweiterungs-Blade 286
Verbindungsmoduleinschübe 286
Bildschirm „Interconnect Bay Summary“ (Zusammenfassung der Verbindungsmoduleinschübe) 286
Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub) 288
Registerkarte „Interconnect Bay Information“ (Informationen zum Verbindungsmoduleinschub) 291
Virtuelle Tasten des Verbindungsmoduleinschubs 293
Bildschirm „Interconnect Bay Port Mapping“ (Portzuordnung des Verbindungsmoduleinschubs) 293
Gehäuse-Power Management 295
Planung für das Power Management 295

Bildschirm „Power and Thermal“ (Stromversorgung und Wärmewerte) 295
Power Management 296
Bildschirm „Enclosure Power Meter“ (Gehäuse-Strommesser) 303
Registerkarte „Graphical View“ (Grafische Ansicht) 304
Registerkarte „Table View“ (Tabellenansicht) 306
Gehäusestromzuordnung 308
Enclosure Power Summary (Gehäusestromversorgung – Zusammenfassung) 308
Bildschirm „Power Subsystem“ (Stromversorgungs-Subsystem) 310
Netzteilinformationen 311
Management von Lüftern und Kühlung 312
Lüfterzonen 312
Thermal Subsystem (Thermisches Subsystem) 313
Regeln zur Lüfterposition für das c7000-Gehäuse 317
Regeln zur Lüfterposition für das c3000-Gehäuse 319
Verwalten von Benutzern 320
Users/Authentication (Benutzer/Authentifizierung) 320
Benutzerrollen und Berechtigungsebenen 320
Rollenbasierte Benutzerkonten 321
Lokale Benutzer 322
Add Local User (Lokalen Benutzer hinzufügen) 323
Edit Local User (Lokalen Benutzer bearbeiten) 323
Registerkarte „Edit Local User Certificate Information“ (Zertifikatinformationen des lokalen Benutzers bearbeiten) 327
Kennworteinstellungen 327
Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 328
Registerkarte „Directory Certificate Information“ (Verzeichniszertifikats-Informationen) 331
Hochladen eines Zertifikats 331
Registerkarte „Directory Certificate Upload“ (Hochladen des Verzeichniszertifikats) 333
Registerkarte „Directory Test Settings“ (Verzeichnis-Testeinstellungen) 333
Verzeichnisgruppen 335
Hinzufügen einer LDAP-Gruppe 337
Bearbeiten einer LDAP-Gruppe 339
SSH-Verwaltung 342
Unterstützte SSH- und SSL-Versionen 343
Integration in HP SSO 343
2-Faktor-Authentifizierung 344
Registerkarte „Two-Factor Authentication Certificate Information“ (Zertifikatinformationen der 2-Faktor-Authentifizierung) 345
Registerkarte „Two-Factor Authentication Certificate Upload“ (Hochladen des Zertifikats der 2-Faktor-Authentifizierung) 346

Angemeldete Benutzer 346
Registerkarte „Session Options“ (Sitzungsoptionen) 347
Insight Display 347
Virtual Connect Manager 348
iLO Integration 348
Managementnetzwerk-IP-Abhängigkeiten 349

9 Verwenden der Befehlszeilenschnittstelle 350
Die Befehlszeilenschnittstelle 350
Einrichten von Onboard Administrator mithilfe der Befehlszeilenschnittstelle 350
Pinbelegungssignale für den seriellen RS232-Anschluss von Onboard Administrator 352
Verwenden der Service-Port-Verbindung 353
Verwenden von Konfigurationsskripts 354
Konfigurationsskripts 354
Werkseinstellungen wiederherstellen 355

10 Unterstützung für HP Integrity i2 Server Blades 357
Aktualisierte Unterstützung für HP Integrity BL860c i2, BL870c i2 und BL890c i2 Server Blades ... 357
Änderungen der Strukturansicht und der grafischen Ansicht für HP Integrity i2 Server Blades 357
Änderungen der Portzuordnung für HP Integrity i2 Server Blades 359
Partner-Blade-Änderungen für HP Integrity i2 Server Blades 359

11 Fehlerbeseitigung 360
Fehlermeldungen im Onboard Administrator 360
Werkseinstellungen von Onboard Administrator 383
Onboard Administrator-SNMP-Traps 383
Bekannte Browser-Probleme 385
Bekannte Netzwerkprobleme 387
Verschiedene bekannte Probleme 387

12 Aktivieren der LDAP-Directory Services-Authentifizierung bei Microsoft Active Directory 390
Zertifizierungsdienste 390
Vorbereiten des Verzeichnisses 390
Hochladen des DC-Zertifikats (optional) 391
Erstellen von Verzeichnisgruppen 394
Testen der Verzeichnisanmeldelösung 395
Fehlerbeseitigung für LDAP auf Onboard Administrator 396

13 Erstellen von Zertifizierungsstellen und Konfigurieren der 2-Faktor-Authentifizierung für lokale Benutzer- und LDAP-Gruppenkonten 398
Einführung 398
Konfigurieren der Verzeichnisse 400
Erstellen eines Verzeichnisses zur Repräsentation einer jeden Zertifizierungsstelle und eines jeden Benutzers 401
Ändern und Speichern einer OpenSSL-Konfigurationsdatei in jedem Zertifizierungsstellenverzeichnis 402
Ändern der Standardverzeichnisse 402
Erstellen einer Stammzertifizierungsstelle 402
Kopieren der OpenSSL-Konfigurationsdatei in das Verzeichnis der Stammzertifizierungsstelle 402
Erstellen des Zertifikats und privaten Schlüssels 402
Erstellen einer kombinierten PEM-Datei aus einem privaten Schlüssel und einem Zertifikat 403
Erstellen untergeordneter Zertifizierungsstellen 404
Erstellen der Verzeichnisse für die untergeordnete Zertifizierungsstelle 404
Bereitstellen von x509-Zertifikatinformationen 404
Erstellen einer Zertifikatsignieranforderung und eines neuen Serverschlüssels 405
Signieren der level1CA-Zertifikatsignieranforderung mit dem Stamm-ZS-Schlüssel 406
Erstellen von Benutzerschlüsseln und Zertifikatsignieranforderungen 406
Erstellen eines Verzeichnisses für die Datenbank der Benutzerschlüssel und Zertifikatsignieranforderungen 407
Bereitstellen von x 509-Benutzerzertifikatinformationen 407
Erstellen einer Benutzer-Zertifikatsignieranforderung und eines neuen Serverschlüssels 407
Signieren der Benutzer-Zertifikatsignieranforderung mit dem level1CA-Schlüssel 408
Überprüfen von Zertifikaten 410
Speichern eines Benutzerzertifikats auf einer Smart Card oder einem Browser 411
Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung anhand lokaler Konten 413
Einrichten eines Onboard Administrator-Wiederherstellungsplans 413
Wiederherstellen über das Insight Display und einen USB-Schlüssel 413
Wiederherstellung über die serielle Konsole 414
Konfigurieren des Onboard Administrator-Sitzungszeitlimits 414
Installieren der Zertifizierungsstellenkette für TFA 415
CLI-Befehle für die Verwaltung von Zertifikaten 418
Konfigurieren des HTTP-Proxy 418
Installieren von Benutzerzertifikaten auf dem lokalen Administratorkonto 418
Aktivieren der 2-Faktor-Authentifizierung 420
Anmelden bei der grafischen Onboard Administrator-Weboberfläche mit der 2-Faktor-Authentifizierung 421

TFA+LDAP-Authentifizierung 421
Wie funktioniert die TFA+LDAP-Authentifizierung 422
Aktivieren der TFA+LDAP-Authentifizierung 422
Methoden zur Angabe des Antragstellerfeldes in einer Zertifikatsignieranforderung 423
Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen 423
CLI-Beispiele für das Konfigurieren eines Benutzerkontos und von Zertifikaten 425
Über das Internet verfügbare Informationen zu Zertifizierungsstellen und Zertifikaten 426

14 Zeitzoneneinstellungen 428
Zeitzoneneinstellungen für die Universalzeit 428
Zeitzoneneinstellungen für Afrika 428
Zeitzoneneinstellungen für Amerika 429
Zeitzoneneinstellungen für Asien 431
Zeitzoneneinstellungen für Ozeanien 432
Zeitzoneneinstellungen für Europa 433
Zeitzoneneinstellungen für Polar-Zeit 433

15 Support und andere Ressourcen 435
Vor der Kontaktaufnahme mit HP 435
HP Kontaktinformationen 435
Weitere Informationen 436

16 Akronyme und Abkürzungen 437

17 Feedback zur Dokumentation 441

Index 442

1 Einführung

Übersicht

HP BladeSystem Onboard Administrator ist die Gehäusemanagementprozessor-, Subsystem- und Firmwarebasis zur Unterstützung des HP BladeSystem c-Class-Gehäuses und aller verwalteten Komponenten im Gehäuse.

Onboard Administrator ermöglicht die zentrale Ausführung grundlegender Verwaltungsaufgaben auf Server Blades oder Switches im Gehäuse. Onboard Administrator führt Konfigurationsschritte für das Gehäuse durch, ermöglicht Laufzeitverwaltung und -konfiguration für die Gehäusekomponenten und informiert Sie über Probleme im Gehäuse per E-Mail, SNMP oder Insight Display.

HP empfiehlt, dass Sie das jeweilige HP BladeSystem c3000 oder c7000-Gehäuse Benutzerhandbuch lesen und sich mit den gehäusespezifischen Eigenschaften vertraut machen, bevor Sie mit dem Onboard Administrator-Setup fortfahren.

HP BladeSystem Onboard Administrator stellt mehrere Funktionen bereit, die die Verwaltung von cClass-Blades und Verbindungsmodulen vereinfachen. Die HP BladeSystem c3000- und c7000-Gehäuse können mit redundanten Onboard Administrator-Modulen konfiguriert werden, um ununterbrochene Verwaltbarkeit des gesamten Gehäuses und der Blades im Fall einer Störung bei einem einzelnen Onboard Administrator-Modul zu bieten. Die folgende Tabelle gibt an, welche Onboard Administrator-Funktion verbessert wird, wenn das Gehäuse redundante Onboard Administrator-Module enthält. In der Tabelle wird das Verhalten für ein Gehäuse mit nur einem einzigen Onboard Administrator-Modul angegeben, wenn dieses Onboard Administrator-Modul ausgefallen ist oder entfernt wurde. Die dynamische Festlegung einer Stromobergrenze für das Gehäuse, die in der Onboard Administrator-Firmwareversion 2.31 eingeführt wurde, ist nur in HP BladeSystem-Gehäusen verfügbar, in denen redundante Onboard Administrator-Module installiert sind.

Vorteile einer redundanten Onboard Administrator-Konfiguration gegenüber einer Konfiguration mit nur einem Onboard Administrator

Onboard Administrator-Funktion	Ein Onboard Administrator im Gehäuse	Ein Onboard Administrator ausgefallen oder entfernt	Redundanter Onboard Administrator im Gehäuse
Stromzuordnung und -steuerung für alle Blades und Verbindungsmodule.	Ja. Keine dynamische Festlegung der Stromobergrenze für das Gehäuse, da für diese Funktion eine redundante Onboard Administrator-Konfiguration erforderlich ist.	Nein. Netzteile versorgen weiterhin alle Blades und Verbindungsmodule mit Strom. Keine Stromversorgung auf Anforderung für Blades oder Verbindungsmodule möglich.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls. Die dynamische Festlegung einer Stromobergrenze für das Gehäuse erfordert eine redundante Onboard Administrator-Konfiguration.
Kühlung aller Blades und Verbindungsmodule.	Ja. Vollständige Steuerung.	Nein. Alle Gehäuselüfter steigern ihre Leistung auf eine unverwaltete höhere Geschwindigkeit, um Blades und Verbindungsmodule vor Überhitzung zu schützen.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.

Onboard Administrator-Funktion	Ein Onboard Administrator im Gehäuse	Ein Onboard Administrator ausgefallen oder entfernt	Redundanter Onboard Administrator im Gehäuse
EBIPA (Enclosure Bay IP Addressing; IP-Adressierung für den Gehäuseeinschub).	Ja. Vollständige Steuerung.	Nein. EBIPA-IP-Adressen gehen nach Lease-Timeout verloren.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.
Ethernet-Verbindungen zu Onboard Administrator, Server-iLO, Verbindungsmanagementprozessoren, z. B. Virtual Connect, die den Onboard Administrator-/iLO-Management-Port verwenden.	Ja. Vollständige Steuerung.	Keine Ethernet-Managementverbindungen, einschließlich des internen Managementverkehrs, z. B. Virtual Connect Manager, mit anderen VC-Modulen im Gehäuse.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.
Informationen und Zustandsberichterstellung für alle Blades, Verbindungsmodule, Lüfter, Netzteile, Onboard Administrator-Module und Gehäuse über die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle von Onboard Administrator, AlertMail oder SNMP.	Ja. Vollständige Steuerung.	Es sind keine Informationen vom Onboard Administrator und auch keine Out-of-Band-Informationen von VCM oder iLO auf einem Server verfügbar.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.
Insight Display	Ja. Vollständige Steuerung.	Nein.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.
Gehäuse-DVD (erfordert entweder c3000-DVD-Option, externes USB-DVD-Laufwerk oder USB-Schlüssel).	Ja. Vollständige Steuerung.	Nein.	Ja. Vollständige Steuerung, einschließlich Aufrechterhaltung des Betriebs bei Ausfall eines Onboard Administrator-Moduls.
Gehäuse-KVM (erfordert c3000 KVM-Option oder Onboard Administrator-Modul mit VGA-Anschluss).	Ja. Vollständige Steuerung.	Nein.	Ja. Vollständige Steuerung. Für das HP c3000-Gehäuse, erfordert sowohl die c3000 KVM-Option als auch die redundante Onboard Administrator-Option. Für das HP c7000-Gehäuse, erfordert zwei der neueren Onboard Administrator-Module mit VGA-Anschluss.

Gespeicherte Onboard Administrator-Einstellungen und Ersatzmodul

Gehäusemodell	Ein Onboard Administrator im Gehäuse	Redundantes Onboard Administrator-Modul (gleicher Ersatztyp installiert)[1]	Redundantes Onboard Administrator-Modul (unterschiedlicher Ersatztyp installiert)[1]
c3000	Alle Gehäuseeinstellungen gehen verloren, wenn ein einzelnes Modul entfernt wird, und müssen manuell über das Insight Display und den USB-Schlüssel, die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle wiederhergestellt werden.	Alle Gehäuseeinstellungen werden auf dem verbleibenden Modul beibehalten und diese Einstellungen werden mit dem ersetzten Modul synchronisiert, sofern die Firmwareversionen übereinstimmen.[2]	Wenn vom nicht redundanten c3000 Onboard Administrator-Modul zum redundanten Onboard Administrator-Modul mit DDR2 gewechselt wird, müssen die Gehäuseeinstellungen manuell über das Insight Display und den USB-Schlüssel, die grafische Benutzeroberfläche oder die Befehlszeilenoberfläche wiederhergestellt werden.
c7000	Alle Gehäuseeinstellungen gehen verloren, wenn ein einzelnes Modul entfernt wird, und müssen manuell über das Insight Display und den USB-Schlüssel, die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle wiederhergestellt werden.	Alle Gehäuseeinstellungen werden auf dem verbleibenden Modul beibehalten und diese Einstellungen werden mit dem ersetzten Modul synchronisiert, sofern die Firmwareversionen übereinstimmen.[2]	Alle Gehäuseeinstellungen werden auf dem verbleibenden Modul beibehalten und diese Einstellungen werden mit dem ersetzten Modul synchronisiert, sofern die Firmwareversionen übereinstimmen.[2]

[1] Wird ein redundantes Onboard Administrator Modul unverzüglich entfernt, wird das verbleibende Modul zum aktiven Onboard Administrator-Modul.

[2] Wenn die Versionen der Onboard Administrator-Firmware nicht übereinstimmen, werden die Einstellungen nicht automatisch synchronisiert. Synchronisieren Sie die Firmware über das Insight Display, die grafische Benutzeroberfläche oder die CLI-Befehlszeilenschnittstelle. Die Einstellungen werden dann automatisch mit dem ersetzten Onboard Administrator-Modul synchronisiert.

Zugriffsanforderungen

Für den Zugriff auf die HP BladeSystem-Onboard Administrator-Webschnittstelle benötigen Sie die IP-Adresse des Onboard Administrator-Moduls sowie einen kompatiblen Web-Browser. Der Zugriff auf die Anwendung muss über HTTPS erfolgen (HTTP-Pakete werden über eine SSL-verschlüsselte Sitzung ausgetauscht).

Für die Weboberfläche von HP BladeSystem-Onboard Administrator ist ein XSLT-fähiger Browser mit Unterstützung für JavaScript 1.3 oder gleichwertig erforderlich.

Eine Liste der für die Verwendung mit Onboard Administrator unterstützten Browser finden Sie in der neuesten Version der Onboard Administrator Versionshinweise.

Vor dem Ausführen des Webbrowsers müssen Sie die folgenden Browser-Einstellungen aktivieren:

- ActiveX (für Microsoft® Internet Explorer)
- Cookies
- JavaScript

Wenn in einer Meldung darauf hingewiesen wird, dass Ihr Browser nicht über die erforderliche Funktionalität verfügt, stellen Sie sicher, dass die Browsereinstellungen die vorstehend genannten

Anforderungen erfüllen, und lesen Sie im Abschnitt „Wiederherstellen des Administratorkennworts“ (Wiederherstellen des Administratorkennworts auf Seite 15) in diesem Handbuch nach.

Wenn ein installiertes Sprachpaket mit der Onboard Administrator-GUI verwendet wird und der Browser nicht alle Zeichen richtig anzeigt, stellen Sie sicher, dass im Betriebssystem die entsprechende Sprachunterstützung installiert wurde.

Für den Zugriff auf die HP BladeSystem-Onboard Administrator-Befehlszeilenschnittstelle verwenden Sie die HP BladeSystem-Onboard Administrator-IP-Adresse sowie ein Terminal oder eine Terminalanwendung. Für den Zugriff auf die Befehlszeilenschnittstelle müssen Sie Telnet oder SSH verwenden, je nachdem, welches dieser Protokolle aktiviert ist.

Die folgenden Ports werden verwendet, um auf den Onboard Administrator zuzugreifen und ihn zu überwachen.

Protokoll	Eingehender Port	Ausgehender Port
SSH	22	—
Telnet	23	—
SMTP	—	25
Browser-Zugriff	80	80
Verschlüsselter Browser-Zugriff	443	443
SNMP Get/Set	161	—
SNMP-Traps	—	162
LDAP SSL	—	636
Globaler LDAP-Katalog	—	3269
Terminaldienste-Durchgang von PC zu iLO	3389	—
iLO Remote Console	17790	—
Virtuelle Medien von PC zu iLO	17988	—
Remote-Systemprotokoll	—	514

Sie können die Portnummern für die LDAP- und Remote-Protokolle ändern.

Wenn ein Protokoll deaktiviert wird, werden die entsprechenden Ports ebenfalls deaktiviert.

Zur Verwendung der dynamischen Stromobergrenze des Gehäuses ist die iLO-Firmware 1.70 oder höher erforderlich.

HINWEIS: Der Onboard Administrator unterstützt mehrere gleichzeitige Anmeldesitzungen über die Onboard Administrator-Weboberfläche oder CLI, außer im Fall von LDAP/Active Directory-Benutzern. Für diese ist nur eine einzige Anmeldesitzung pro Benutzer zulässig.

Übersicht über Onboard Administrator

Die Verwaltung eines c-Class-Gehäuses umfasst mehrere Funktionen:

- Erkennen eingesetzter und entfernter Komponenten
- Identifizieren von Komponenten einschließlich der benötigten Verbindung

- Verwaltung der Stromversorgung und Kühlung
- Steuerung der Komponenten einschließlich Fernsteuerung und Fernkonsolen

Erkennen eingesetzter und entfernter Komponenten

Onboard Administrator ermöglicht die Komponentensteuerung in c-Class-Gehäusen.
Die Komponentenverwaltung beginnt nach dem Erkennen und Identifizieren der Komponente. Onboard Administrator erkennt Komponenten in BladeSystem c-Class-Gehäusen anhand der Anwesenheitssignale an jedem Einschub. Wenn Sie eine Komponente in einen Einschub einsetzen, erkennt und identifiziert Onboard Administrator die Komponente sofort. Wenn Sie eine Komponente aus einem Einschub entfernen, löscht Onboard Administrator die Informationen über die betreffende Komponente.

Identifizieren von Komponenten

Zum Identifizieren einer Komponente liest Onboard Administrator ein FRU EEPROM, das spezielle Werksinformationen über die Komponente enthält, wie z. B. Produktname, Teilenummer und Seriennummer. Alle FRU EEPROMs in c-Class-Gehäusen werden eingeschaltet, auch wenn die Komponente ausgeschaltet ist. Deshalb kann Onboard Administrator vor dem Gewähren der Stromzufuhr die Komponente identifizieren. Bei Geräten wie Lüftern, Netzteilen und dem Insight Display kann Onboard Administrator die FRU EEPROMs direkt lesen. Auf die FRU EEPROMs von Server Blades greift Onboard Administrator dagegen über iLO-Managementprozessoren zu.

- Die Server Blades enthalten mehrere FRU EEPROMs: eines auf der Serverkarte mit Informationen zum Server und integrierten NIC und eines auf jeder installierten optionalen Mezzanine Card.
- Zu den Server Blade-Steueroptionen gehören die automatische Anmeldung bei der iLO-Webbenutzeroberfläche und den Remote-Server-Konsolen, die virtuelle Steuerung der Stromversorgung und die Steuerung der Bootreihenfolge. Die Server Blade-Steueroptionen umfassen zudem umfangreiche Server-Hardware-Informationen, darunter BIOS und iLO-Firmwareversionen, Servername, NIC- und Optionskarten-Port-IDs und Portzuordnung.
- Onboard Administrator bietet leicht verständliche Portzuordnungsinformationen für jeden Server Blade und jedes Verbindungsmodul im Gehäuse.

Die FRU-Informationen zum NIC und zur optionalen Mezzanine Card teilen Onboard Administrator mit, welche Art von Verbindungsmodulen jeder Server benötigt. Bevor ein Server Blade mit Strom versorgt wird, vergleicht Onboard Administrator diese Informationen mit den FRU EEPROMs auf installierten Verbindungsmodulen, um auf elektronische Eingabefehler zu prüfen.
Bei Verbindungsmodulen ermöglicht Onboard Administrator eine virtuelle Steuerung der Stromversorgung, dedizierte serielle Konsolen und Ethernet-Managementverbindungen.

Beim Start des aktiven Onboard Administrator wird ein Fortschrittsmesser mit 16 Schritten angezeigt. Manche Schritte können mehrere Minuten in Anspruch nehmen, je nach Anzahl und Typen der Blades, Mezzanine-Cards und Verbindungsmodule.

Verwaltung der Stromversorgung und Kühlung

Die wichtigsten Aufgaben von Onboard Administrator sind die Steuerung der Stromversorgung und das thermische Management. Onboard Administrator kann den Stromversorgungszustand aller Komponenten in BladeSystem c-Class-Gehäusen remote steuern. Bei den Komponenten in den Geräteeinschüben vorne in jedem Gehäuse kommuniziert Onboard Administrator mit iLO zur Steuerung der Server und mit einem Mikrocontroller zur Steuerung von Optionen wie Speicher-Blades. Ein separater Mikrocontroller steuert die Stromversorgung der Verbindungsmodule.

Nachdem die Komponenten eingeschaltet wurden, beginnt Onboard Administrator mit dem thermischen Management mittels „Thermal Logic“. Die Funktion „Thermal Logic“ in BladeSystem c-Class minimiert den Stromverbrauch des Lüfter-Subsystems des Gehäuses, indem sie über das

gesamte Gehäuse hinweg Temperatursensoren abliest. Dann ändert Thermal Logic die Lüftergeschwindigkeit in verschiedenen Zonen im Gehäuse, um den Stromverbrauch zu minimieren und die Kühlungseffizienz zu maximieren.

Steuern von Komponenten

Onboard Administrator verwendet integrierte Managementschnittstellen, um ausführliche Informationen und Zustandsangaben für alle Einschübe im Gehäuse bereitzustellen, einschließlich Präsenzerkennungssignale für alle Einschübe, i2c, serielle Schnittstellen, USB-Ports und Ethernet-Controller. Onboard Administrator macht außerdem Angaben zu den Firmwareversionen der meisten Komponenten im Gehäuse und kann zur Aktualisierung dieser Komponenten verwendet werden.

Schnittstellen

Jedes c-Class-Gehäuse verfügt über mehrere externe Managementschnittstellen, die den Benutzer mit Onboard Administrator verbinden. Die RJ-45-Ethernet-Buchse ist die primäre Schnittstelle. Diese Schnittstelle stellt den Netzwerkzugriff auf den Onboard Administrator und die Verwaltungsschnittstelle auf allen Server Blades (iLO), Speicher-Blades (TBM) und Verbindungsmodulen bereit.

Ein serieller Port auf dem Onboard Administrator-Modul ermöglicht uneingeschränkten bandexternen Befehlszeilenschnittstellenzugriff auf den Onboard Administrator und wird zur Flash-Wiederherstellung der Onboard Administrator-Firmware verwendet.

USB-Ports auf Onboard Administrator werden verwendet, um externe DVD-Laufwerke anzuschließen und die DVD-Funktion des Gehäuses zu unterstützen. Außerdem können Sie ein optionales internes DVD-Laufwerk für das c3000-Gehäuse bestellen. Auf dem USB-Port des Onboard Administrator-Moduls befindet sich möglicherweise ein Aufkleber mit dem Hinweis, dass er zur zukünftigen Verwendung reserviert ist. Um den USB-Port mit der Firmwareversion 2.00 oder höher von Onboard Administrator zu verwenden, entfernen Sie den Aufkleber.

Alle c-Class-Gehäuse unterstützen zwei Gehäuse-Verbindungsanschlüsse, die eine private Kommunikation zwischen Gehäusen ermöglichen, die über ein CAT5-Kabel miteinander verbunden sind. Der Gehäuse-Link-up-Anschluss verfügt über einen Service-Port, über den Sie zur lokalen Diagnose und Fehlersuche vorübergehend einen Laptop-PC an das Onboard Administrator-Modul eines verknüpften Gehäuses anschließen können.

Die KVM-Modul-Option für das c3000-Gehäuse wird in den hinteren Einschub neben Verbindungsmodul 1 eingesteckt und stellt einen VGA-Anschluss und zwei weitere USB-Anschlüsse für das c3000-Gehäuse bereit. Dieses KVM-Modul aktiviert die Gehäuse-KVM-Funktion für das c3000-Gehäuse. Der VGA-Anschluss wird mit einem externen VGA-Monitor und einer externen USB-Tastatur und -Maus verbunden und bietet so Zugriff auf alle Servervideokonsolen oder die Onboard Administrator-Befehlszeilenschnittstelle oder Insight Display.

Das neue c7000-Onboard Administrator-Modul mit KVM fügt dem c7000-Onboard Administrator einen VGA-Anschluss hinzu und aktiviert die KVM-Funktion für das c7000-Gehäuse. Das aktive c7000-Onboard Administrator-Modul mit KVM bietet die gleichen KVM-Gehäusefunktionen wie das optionale c3000 KVM-Modul. Für parallele Gehäuse-KVM- und Gehäuse-DVD-Funktionen muss ein externer USB-Hub (nicht im Lieferumfang enthalten) verwendet werden, um ein USB-DVD-Laufwerk gleichzeitig mit der KVM-USB-Option für Tastatur und Maus anzuschließen. Das Onboard Administrator Standby-Modul mit KVM bietet nur Zugriff auf die Anmeldung über die Onboard Administrator-Befehlszeilenschnittstelle, die es den angemeldeten Benutzern ermöglicht, eine Übernahme zu erzwingen.

Jedes c-Class-Gehäuse besitzt auf der Vorderseite ein integriertes Insight Display, das Status und Informationen für alle Einschübe in einem c-Class-Gehäuse sowie Diagnoseinformationen bereitstellt, wenn Onboard Administrator ein Problem im Gehäuse erkennt. Das Insight Display konfiguriert die

Haupteinstellungen in Onboard Administrator, einschließlich der IP-Adresse von Onboard Administrator.

Onboard Administrator-Authentifizierung

Durch die Benutzerauthentifizierung wird für alle Onboard Administrator-Benutzeroberflächen die Sicherheit aufrechterhalten. In Onboard Administrator erstellten Benutzerkonten wird eine von drei Berechtigungsebenen zugewiesen und Zugriff auf Komponenteneinschübe entsprechend der angegebenen Berechtigungsstufe gewährt. Onboard Administrator speichert die Kennwörter für lokale Benutzerkonten und kann für die LDAP-Authentifizierung von Benutzergruppenkonten konfiguriert werden. Das Insight Display kann durch einen LCD-Pin-Code geschützt oder vollständig deaktiviert werden. Ein LCD-PIN-Code schützt vor nicht berechtigtem Zugriff auf das Insight Display und die Gehäuse-KVM. Die Verwendung des KVM-Moduls für den Zugriff auf Serverkonsolen wird durch Benutzernamen und Kennwörter im Serverbetriebssystem geschützt.

HINWEIS: Onboard Administrator unterstützt nicht OpenLDAP.

Rollenbasierte Benutzerkonten

Onboard Administrator stellt konfigurierbare Benutzerkonten bereit, die die vollständige Trennung mehrerer Administratorrollen, z. B. Server, LAN und SAN, ermöglichen. Benutzerkonten werden mit bestimmten Geräteeinschubs- oder Verbindungsmoduleinschubs-Berechtigungen und einer von drei Berechtigungsebenen konfiguriert: Administrator, Bediener oder Benutzer. Ein Konto mit Administratorrechten für die Onboard Administrator-Einschubberechtigung kann alle Benutzerkonten für ein Gehäuse erstellen oder bearbeiten. Bedienerberechtigungen ermöglichen den uneingeschränkten Informationszugriff und die Steuerung erlaubter Einschübe. Benutzerberechtigungen erlauben den Informationszugriff, jedoch nicht die Steuerung.

Zur Verwendung von Onboard Administrator müssen Sie sich über die grafische Benutzeroberfläche oder die Befehlszeilenschnittstelle mit einem Konto und einem Kennwort an der Webschnittstelle anmelden. Ist das Konto ein lokales Konto, ist das Kennwort auf Onboard Administrator gespeichert. Ist das Konto ein LDAP-Konto, überprüft Onboard Administrator die Anmeldeinformationen des Benutzers auf dem festgelegten LDAP-Server. Die 2-Faktor-Authentifizierung ermöglicht eine sogar noch strengere Sicherheit für Benutzerverwaltungssitzungen mit Onboard Administrator. Es ist auch möglich, sowohl die 2-Faktor-Authentifizierung als auch die LDAP-Authentifizierung zu konfigurieren, wie unter „TFA+LDAP-Authentifizierung“ (TFA+LDAP-Authentifizierung auf Seite 421) beschrieben.

Anstatt separate Anmeldungen bei mehreren Ressourcen vorzuschreiben (einmal bei jedem Gehäuse und/oder einmal bei jedem Servermanagementprozessor) ermöglicht Onboard Administrator im Fall verbundener Gehäuse in einem Rack den Zugriff über über einen einzelnen Punkt. So kann sich der Administrator mit der Funktion der einmaligen Anmeldung bei einem einzelnen Onboard Administrator-Modul anmelden und die grafische Weboberfläche verwenden, um die HP BladeSystem c-Class-Komponenten in bis zu sieben miteinander verbundenen Gehäusen grafisch darzustellen und zu verwalten. (Für die einmalige Anmeldung müssen alle aktiven Onboard Administrator-Module des Gehäuses über das gleiche Kennwort verfügen.) Beispiel: Ein IT-Administrator kann Verwaltungsbefehle, wie z. B. das Ändern des Gehäuse-Stromversorgungsmodus, automatisch über alle verbundenen Gehäuse hinweg verbreiten. Für die einzelnen verbundenen Gehäuse muss ein gültiges Konto vorhanden sein, um Zugriff zu erhalten. Weitere Informationen finden Sie unter „Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator“ (Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator auf Seite 10).

Anmeldesicherheit

Onboard Administrator bietet mehrere Anmeldesicherheitsfunktionen. Der erste fehlgeschlagene Anmeldeversuch wird nicht bestraft. Bei allen nachfolgenden fehlgeschlagenen Versuchen verhängt Onboard Administrator eine 10- bis 30-sekündige Verzögerung. Während jeder Verzögerung wird

eine Informationsseite angezeigt. Dieser Ablauf wiederholt sich, bis gültige Anmeldedaten eingegeben werden. Diese Funktion hilft, vor möglichen Dictionary-Angriffen zu schützen.

Onboard Administrator speichert für alle fehlgeschlagenen Anmeldeversuche jeweils einen detaillierten Protokolleintrag.

Erstmaliges Ausführen von Onboard Administrator

Die Einrichtung eines c-Class-Gehäuses mithilfe von Onboard Administrator wird durch den Assistenten von Insight Display für die Erstinstallation vereinfacht, gefolgt vom Assistenten für die Erstinstallation der grafischen Benutzeroberfläche von Onboard Administrator oder der Onboard Administrator-Befehlszeilenschnittstelle, um die Gehäuseeinstellungen zurückzusetzen.

Bei Betrieb im FIPS-Modus muss der FIPS-Modus zuerst vor Vornahme jeder anderen Gehäuse- oder Onboard Administrator-Konfiguration, einschließlich der Konfiguration von Virtual Connect oder dem Assistenten für die Erstkonfiguration, konfiguriert werden. Wenn der FIPS-Modus auf einem Onboard Administrator-Modul oder einem redundanten Paar von Modulen aktiviert wird, wird ein Zurücksetzen der Onboard Administrator-Module auf die Werkseinstellungen erzwungen. Nachdem der FIPS-Modus konfiguriert wurde, führen Sie die Konfigurationsschritte in diesem Abschnitt aus. Weitere Informationen zum FIPS-Modus finden Sie unter „Registerkarte ‚FIPS‘“ (Registerkarte „FIPS“ auf Seite 140).

Als Management-IP-Adresse von Onboard Administrator-Modulen, Server Blade-iLO-Managementprozessoren und vielen Verbindungsmodulen wird standardmäßig DHCP festgelegt. Wenn der Benutzer über DHCP verfügt und den Onboard Administrator-Management-Port mit dem DHCP-Server verbindet, rufen alle Onboard Administrator-Module, iLO-Module und Verbindungsmodule, die die Verwendung des internen Managementnetzwerks von Onboard Administrator unterstützen und entsprechend konfiguriert sind, automatisch DHCP-Adressen vom Benutzer-DHCP-Server ab.

Wenn Sie über keinen DHCP-Server verfügen, um Managementprozessoren IP-Adressen zuzuweisen, müssen Sie jede Onboard Administrator-IP-Adresse und anschließend alle einzelnen Komponenten- und Verbindungsmodulmanagement-IP-Adressen mit einer der folgenden Methoden konfigurieren:

- Empfohlene Vorgehensweise: Konfigurieren Sie Onboard Administrator über das Insight Display mit einer statischen IP-Adresse. Melden Sie sich dann an der grafischen Benutzeroberfläche von Onboard Administrator an, und verwenden Sie den Assistenten für die Erstkonfiguration (First Time Setup Wizard), oder melden Sie sich an der Onboard Administrator-Befehlszeilenschnittstelle an, und konfigurieren und aktivieren Sie Enclosure Bay IP Addresses (EBIPA) für Geräteeinschübe und Verbindungsmoduleinschübe. Durch das Aktivieren von EBIPA für einen Einschub ist es möglich, den Server oder das Verbindungsmodul zu ersetzen, und das neue Modul erhält automatisch die zuvor konfigurierte IP-Adresse für diesen Einschub.
- Alternativ können Sie jede Komponente und jedes Verbindungsmodul für statische IP-Adressen manuell konfigurieren. Für ProLiant Server Blades müssen Sie über den SUV-Port eine Verbindung mit jedem Server Blade in SUV herstellen (mithilfe des in jedem Gehäuse vorhandenen SUV-Kabels) und die iLO-IP-Adresse manuell während des POST konfigurieren, indem Sie F8 drücken, um die iLO-Option-ROM-Einstellungen aufzurufen. Für die Verbindungsmodule mit Managementprozessoren, die das Onboard Administrator-Managementnetzwerk verwenden können, rufen Sie die IP-Adresse über einen externen seriellen Konsolenport oder die serielle Verbindung der Onboard Administrator-Befehlszeilenschnittstelle zu diesem Einschub auf und konfigurieren diese. Nach dem manuellen Ändern der Verbindungsmodul-IP-Adresse verlangt der Switch möglicherweise das Aus- und Wiedereinschalten, damit die neue Einstellung wirksam wird.

HINWEIS: Die IP-Adresse für einen Onboard Administrator darf nicht im Bereich 169.254.x.x konfiguriert werden.

Die ursprünglichen Anmeldeinformationen für ein neues Onboard Administrator-Modul stehen auf einem Etikett, das sich auf jedem Modul befindet. Der Benutzer ist Administrator, und das Kennwort ist für jedes Modul eindeutig. Dieses Kennwort muss vom Installationsprogramm aufgezeichnet werden und dem Remote-Administrator für die erste Remote-Anmeldung an der grafischen Benutzeroberfläche von Onboard Administrator oder der Onboard Administrator-Befehlszeilenschnittstelle mitgeteilt werden.

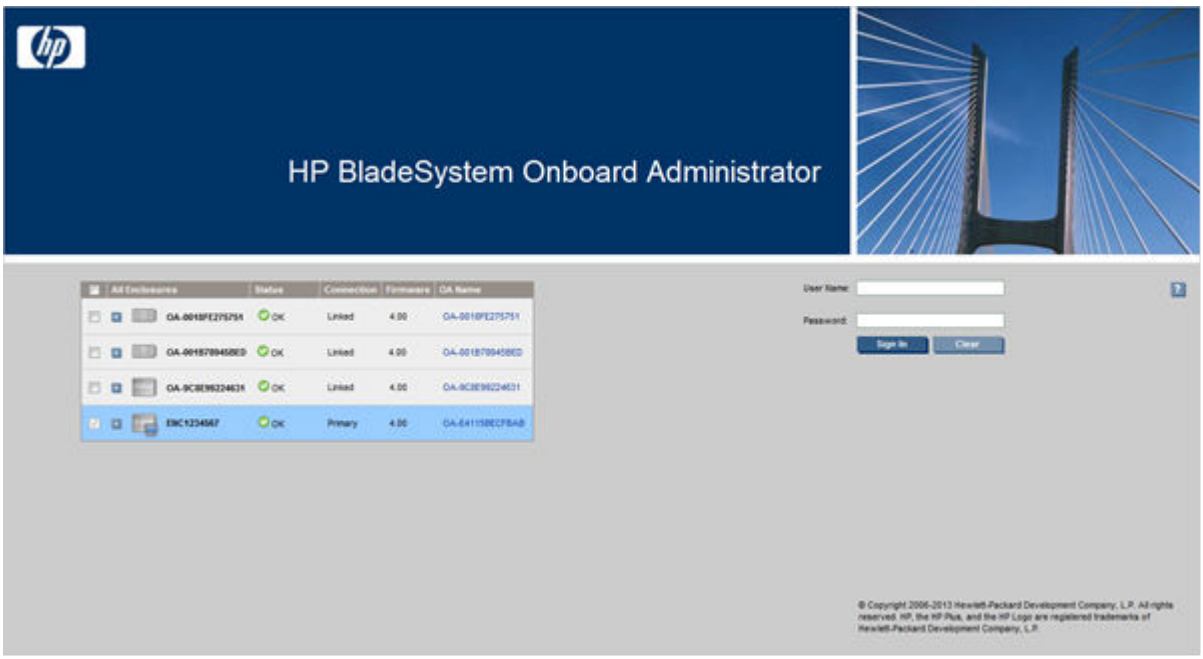
Die Gehäuseeinstellungen können manuell konfiguriert oder von einem Konfigurationsskript oder einer Datei hochgeladen werden. Die grafische Benutzeroberfläche der Webschnittstelle besitzt einen Assistenten für die Erstkonfiguration (First Time Setup Wizard). Der Zugriff auf die Befehlszeilenschnittstelle ist über den seriellen Port von Onboard Administrator, den Ethernet-Management-Port, den Service-Port oder die Schaltfläche für die Gehäuse-KVM-Befehlszeilenschnittstelle von Onboard Administrator möglich.

Eine Alternative zur manuellen Konfiguration ist das Hochladen einer Gehäusekonfigurationsdatei auf den aktiven Onboard Administrator über die grafische Benutzeroberfläche, die Befehlszeilenschnittstelle oder das Insight Display mit einem HTTP-, FTP- oder TFTP-Netzwerkpfad zur Konfigurationsdatei oder das Hochladen einer Konfigurationsdatei von einem an den USB-Port des aktiven Onboard Administrator-Moduls angeschlossenen USB-Schlüssellaufwerk über die grafische Benutzeroberfläche, die Befehlszeilenschnittstelle oder das Insight Display.

Die empfohlene Vorgehensweise für die Erstellung einer Gehäusekonfigurationsdatei ist die Verwendung der grafischen Benutzeroberfläche, der Befehlszeilenschnittstelle oder des Insight Display „USB Key Menu“ (USB-Schlüssel-Menü), um die vorhandene Konfiguration in einer Datei zu speichern. Die gespeicherte Konfigurationsdatei besteht aus Befehlszeilenschnittstellen-Textbefehlen für jedes Konfigurationselement. Onboard Administrator speichert keine Benutzerkennwörter beim Speichern einer Konfigurationsdatei. Der Benutzer kann die Konfigurationsdatei bearbeiten und die Kennwortbefehle für jedes Benutzerkonto einfügen oder das lokale Administratorkonto verwenden, um alle Benutzerkennwörter einzeln zu aktualisieren, nachdem eine zuvor gespeicherte Gehäusekonfigurationsdatei wiederhergestellt wurde.

Wenn das Gehäuse redundante Onboard Administrator-Module enthält, aktualisiert der verbleibende Onboard Administrator den neuen Onboard Administrator mit allen Einstellungen.

Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator



Geben Sie den Benutzernamen und das ursprüngliche Administratorkennwort für das Onboard Administrator-Modul ein. Die Standard-Anmeldeinformationen finden Sie auf dem Etikett auf dem Onboard Administrator-Modul.

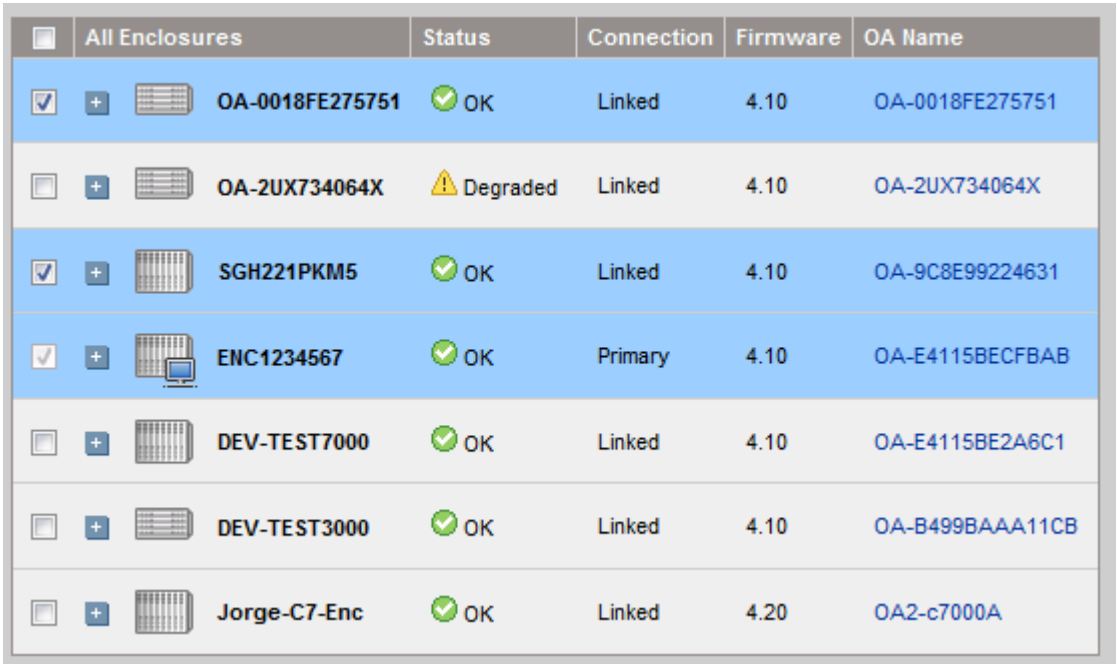
Bei der Anmeldung bei dem Onboard Administrator können die folgenden Probleme auftreten:

- Sie haben die Informationen nicht richtig eingegeben. Die Groß-/Kleinschreibung des Kennworts wird berücksichtigt.
- Die eingegebenen Kontoinformationen wurden nicht für HP BladeSystem Onboard Administrator konfiguriert.
- Der angegebene Benutzername wurde gelöscht, deaktiviert oder gesperrt.
- Das Kennwort für das Konto muss geändert werden.
- Sie versuchen, sich über eine IP-Adresse anzumelden, die für das betreffende Konto nicht gültig ist.
- Sie können sich nicht an das Kennwort für das Administratorkonto erinnern oder haben es verlegt. Anweisungen zum Zurücksetzen des Administratorkennworts finden Sie unter „Wiederherstellen des Administratorkennwortes“ (Wiederherstellen des Administratorkennworts auf Seite 15).

Wenn die Probleme weiterhin bestehen, wenden Sie sich an Ihren Administrator.

Wenn Sie auf mehreren Gehäusen die gleichen Anmeldeinformationen verwenden, können Sie sich mit der einmaligen Anmeldung bei mehreren miteinander verbundenen Gehäusen anmelden. Aktivieren Sie vor der Anmeldung das Kontrollkästchen eines jeden verknüpften Gehäuses, das in der Tabelle auf der Seite „Sign-in“ (Anmelden) aufgelistet wird, wie in der folgenden Tabelle dargestellt. In diesem Szenario versuchen Sie sich mit dem bereitgestellten Benutzernamen und Kennwort bei drei aktiven Onboard Administrator-Modulen auf den entsprechenden ausgewählten Gehäusen anzumelden. Wenn die Überprüfung und Anmeldung bei allen miteinander verbundenen Gehäusen erfolgen soll, können Sie alternativ dazu das Kontrollkästchen oben in der Spalte der

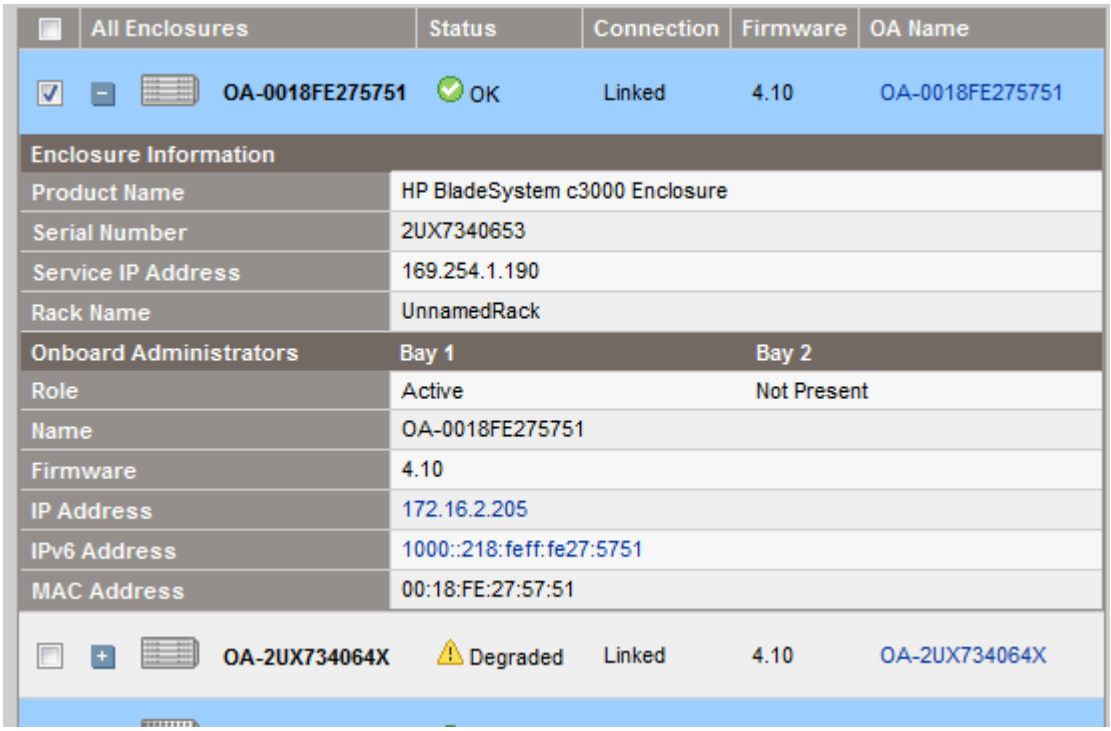
Kontrollkästchen aktivieren. Bei erfolgreicher Anmeldung wird jedes dieser Gehäuse im gleichen Fenster der grafischen Benutzeroberfläche angezeigt. Die Anzeigereihenfolge der einzelnen Gehäuse basiert auf den Gehäuse-Link-Kabeln. Verbinden Sie den „Abwärts-Link“-Port des obersten Gehäuses mit dem „Aufwärts-Link“-Port des folgenden Gehäuses. Wiederholen Sie dies, bis Sie das unterste Gehäuse erreicht haben. Diese Reihenfolge auf der grafischen Benutzeroberfläche entspricht der im CLI-Befehl `SHOW TOPOLOGY` verwendeten Reihenfolge.



All Enclosures	Status	Connection	Firmware	OA Name
OA-0018FE275751	OK	Linked	4.10	OA-0018FE275751
OA-2UX734064X	Degraded	Linked	4.10	OA-2UX734064X
SGH221PKM5	OK	Linked	4.10	OA-9C8E99224631
ENC1234567	OK	Primary	4.10	OA-E4115BECFBAB
DEV-TEST7000	OK	Linked	4.10	OA-E4115BE2A6C1
DEV-TEST3000	OK	Linked	4.10	OA-B499BAAA11CB
Jorge-C7-Enc	OK	Linked	4.20	OA2-c7000A

Wie im voranstehenden Beispiel ersichtlich, enthält die Gehäusetabelle auch Informationen zum Gehäusestatus, zur Verbindung, zur Firmwareversion, zum OA-Namen und zur Rack-Position. Wurden auf der Registerkarte „Anonymous Data“ (Anonyme Daten) der Seite „Network Access“ (Netzwerkzugriff) erweiterte Daten aktiviert, dann können Sie detaillierte Gehäuse- und Onboard Administrator-Daten durch Auswahl des Zeichens + links neben dem Gehäusesymbol anzeigen. Das Zeichen + erscheint nur, wenn auf dem betreffenden Gehäuse erweiterte Daten aktiviert sind. Mittels der Positionsermittlungsdienste (Location Discovery Services) enthalten die erweiterten Daten Positionsinformationen für jedes Chassis. Weitere Informationen zu den Positionsermittlungsdiensten (Location Discovery Services) finden Sie unter „Bildschirm ‚Rack Overview‘ (Rack-Übersicht)“ (Bildschirm „Rack Overview“ (Rack-Übersicht) auf Seite 100). Die erweiterten Daten sind standardmäßig aktiviert. Sind auf einem Gehäuse erweiterte Daten deaktiviert, wird der Status des betreffenden Gehäuses als `N/A` (Nicht zutreffend) angegeben.

Die folgende Abbildung zeigt die erweiterten Daten für das erste in der Tabelle aufgelistete Gehäuse.



Flash-Notfallwiederherstellung

Um einen Onboard Administrator nach einem fehlgeschlagenen Flash-Verfahren wiederherzustellen, wird Folgendes benötigt:

- Lokaler Zugriff auf das Gehäuse
- Ein für den Onboard Administrator zugänglicher DHCP-Server
- Ein für den Onboard Administrator zugänglicher TFTP-Server
- Onboard Administrator-Firmware (.bin-Datei)

Stellen Sie Onboard Administrator nach einer fehlgeschlagenen Flash-Wiederherstellung mit einem der folgenden Verfahren wieder her:

- Wenn sich im Gehäuse nur ein Onboard Administrator-Modul befindet oder die Flash-Wiederherstellung bei dem aktiven OA-Modul vorgenommen werden soll:

  a. Stellen Sie eine lokale Verbindung zum Onboard Administrator-Modul über ein Nullmodemkabel (9600 N, 8, 1, VT100) her.

  b. Drücken und halten Sie die Taste zum Zurücksetzen am Onboard Administrator-Modul 5 Sekunden lang gedrückt.

  c. An der seriellen Konsole werden Sie zur Auswahl der Option „Flash Recovery“ (Flash-Wiederherstellung) oder „Reset Password“ (Kennwort zurücksetzen) aufgefordert. Drücken Sie **F**. Onboard Administrator erhält eine IP-Adresse über DHCP.

  d. Geben Sie an der Eingabeaufforderung für die IP-Adresse des TFTP-Servers (Speicherort der Image-Dateien von Onboard Administrator) die entsprechende IP-Adresse ein.

  e. Sie werden zur Eingabe des Pfads zum Onboard Administrator-Firmware-Image aufgefordert. Onboard Administrator lädt das Image herunter und flasht sich selbst.

Nachdem dieser Vorgang erfolgreich abgeschlossen wurde, befindet sich die Onboard Administrator-Firmware auf dem neuesten Stand und alle Fehlerbedingungen wurden behoben.

- Wenn sich im Gehäuse zwei Onboard Administrator-Module befinden und eine Flash-Wiederherstellung des aktiven OA-Moduls vorgenommen werden soll:

  a. Stellen Sie eine lokale Verbindung zum Onboard Administrator-Modul über ein Nullmodemkabel (9600 N, 8, 1, VT100) her.

  b. Drücken und halten Sie die Taste zum Zurücksetzen am Onboard Administrator-Modul 5 Sekunden lang gedrückt.

  c. Wenn Sie an der seriellen Konsole zur Auswahl der Option „Flash Recovery“ (Flash-Wiederherstellung) oder „Reset Password“ (Kennwort zurücksetzen) aufgefordert werden, machen Sie keine Eingabe. Warten Sie mindestens 2 Minuten oder länger, um das OA-Standby-Modul zum aktiven OA-Modul werden zu lassen, bevor Sie mit dem nächsten Schritt fortfahren.

  d. Wenn das OA-Modul, das geflasht werden soll, zum OA-Standby-Modul geworden ist, drücken und halten Sie die Taste zum Zurücksetzen an dem selben OA-Modul wie in Schritt b ein zweites Mal.

  e. An der seriellen Konsole werden Sie zur Auswahl der Option „Flash Recovery“ (Flash-Wiederherstellung) oder „Reset Password“ (Kennwort zurücksetzen) aufgefordert. Drücken Sie **F**. Onboard Administrator erhält eine IP-Adresse über DHCP.

  f. Geben Sie an der Eingabeaufforderung für die IP-Adresse des TFTP-Servers (Speicherort der Image-Dateien von Onboard Administrator) die entsprechende IP-Adresse ein.

  g. Sie werden zur Eingabe des Pfads zum Onboard Administrator-Firmware-Image aufgefordert. Onboard Administrator lädt das Image herunter und flasht sich selbst.

Nachdem dieser Vorgang erfolgreich abgeschlossen wurde, befindet sich die Onboard Administrator-Firmware auf dem neuesten Stand und alle Fehlerbedingungen wurden behoben.

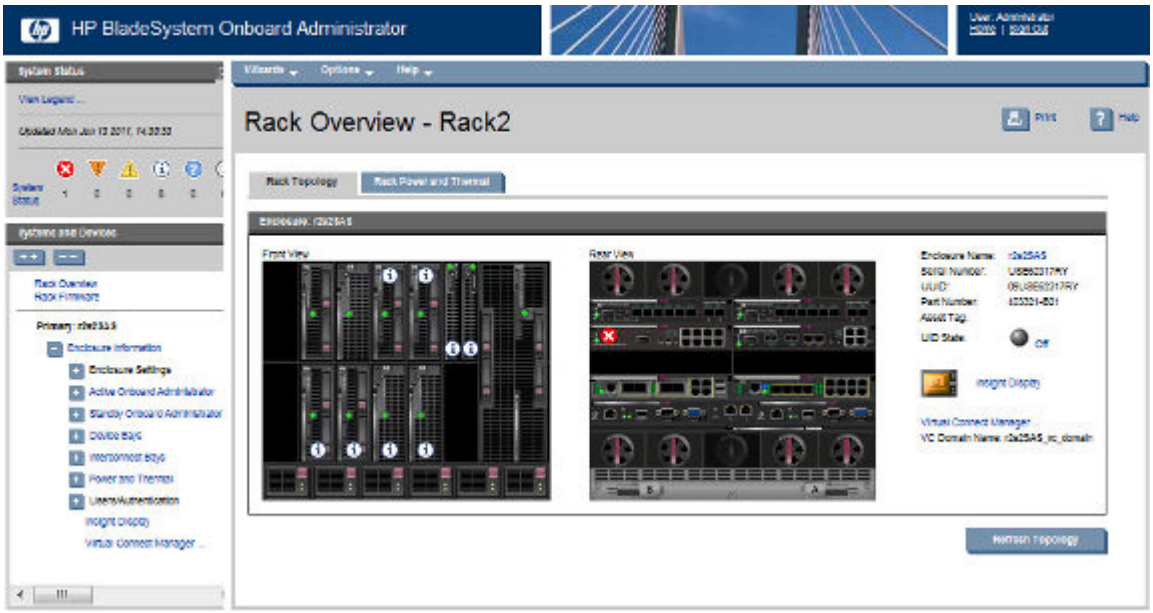
Ausführen des Konfigurationsassistenten

Melden Sie sich zum Ausführen des Konfigurationsassistenten bei Onboard Administrator an. Der Assistent für die Erstkonfiguration „First Time Setup Wizard“ wird automatisch aufgerufen, wenn Sie sich zum ersten Mal bei Onboard Administrator anmelden. Dieser Assistent unterstützt Sie bei der Konfiguration sämtlicher Funktionen von Onboard Administrator. Sie können den Konfigurationsassistenten jederzeit nach der Erstkonfiguration aufrufen, indem Sie auf den Link **Wizards** (Assistenten) oben links im mittleren Bildschirm klicken.

Detaillierte Informationen finden Sie unter „First Time Setup wizard (Assistent für die Erstkonfiguration)“ („Assistent für die Erstkonfiguration (First Time Setup Wizard)“ auf Seite 55).

Verwenden der Online-Hilfe

Die Online-Hilfe erreichen Sie, indem Sie auf das blaue Kästchen mit dem weißen Fragezeichen rechts oben im Bildschirm oder auf **Help** (Hilfe) rechts oben im Bildschirm unter der Kopfleiste klicken. Die Informationen, die in der Online-Hilfe angezeigt werden, beziehen sich auf den Abschnitt von Onboard Administrator, in dem Sie sich gerade befinden.



Ändern von Gehäuse- und Komponentenkonfigurationen

Nachdem Sie den Assistenten für die Erstkonfiguration „First Time Setup Wizard“ beendet haben, können Sie jederzeit zur grafischen Benutzeroberfläche von Onboard Administrator zurückkehren, um Konfigurationsänderungen vorzunehmen. Unter „Konfigurieren des HP BladeSystem c7000-

Gehäuses und von Gehäusekomponenten“ („Konfigurieren von HP BladeSystem-Gehäusen und Gehäusekomponenten“ auf Seite 110) finden Sie Informationen, durch die Änderungen an den Gehäuse- und Gerätekonfigurationen, den Benutzereinstellungen sowie den LDAP-Servereinstellungen und den LDAP-Gruppen erleichtert werden.

Informationen zu den Stromversorgungseinstellungen des Gehäuses finden Sie unter „Enclosure Power Management (Gehäuse-Stromverwaltung)“ (Gehäuse-Power Management auf Seite 295).

Wiederherstellen des Administratorkennworts

Falls Sie das Administratorkennwort verloren haben, können Sie es auf den werkseitigen Standard zurücksetzen, der auf dem Etikett mit dem Onboard Administrator-Modul geliefert wurde. Onboard Administrator setzt ein verloren gegangenes Kennwort auf den Modus „Lost Password/Flash Disaster Recovery (LP/FDR)“ (Verlorenes Kennwort/Flash-Notfallwiederherstellung (LP/FDR)) zurück. So setzen Sie das Administratorkennwort auf die werksseitige Einstellung zurück:

1. Schließen Sie einen Computer über ein Nullmodemkabel an die serielle Schnittstelle des aktiven Onboard Administrator-Moduls an.
2. Stellen Sie eine lokale Verbindung zum Onboard Administrator-Modul über ein Nullmodemkabel (9600 N, 8, 1, VT100) her.
3. Öffnen Sie ein geeignetes Terminalfenster-Programm (Windows oder Linux) und stellen Sie eine Verbindung mit dem Active Onboard Administrator her.
4. Drücken und halten Sie die Taste zum Zurücksetzen im Onboard Administrator 5 Sekunden lang gedrückt.
5. Um das System im Modus „Lost Password“ (Verlorenes Kennwort) zu starten, drücken Sie **L**. Das Kennwort wird bei dem Neustart des Systems angezeigt.

Alternativ können Sie die USB-Option von Insight Display (LCD-Bedienfeld) auswählen, um das Kennwort für das Onboard Administrator-Modul zurückzusetzen. Diese Option stellt mittels Befehlszeilenschnittstellen-Befehlen ein Konfigurationsskript wieder her, das auf einem USB-Schlüssel gespeichert wurde.

HINWEIS: Wenn die USB-Menüschaltflächen von Insight Display gesperrt sind, muss das Verfahren mittels serieller Ports verwendet werden. Wenn das LCD-Bedienfeld gesperrt ist, wird ein großes „Sperrsymbol“ auf dem Bildschirm angezeigt.

In diesem Beispiel wurde das OA-Administratorkennwort als `Password123` festgelegt.

1. Erstellen Sie eine Textdatei mit dem Namen `reset_password.cfg`, das folgenden einzeiligen Befehl enthält: `SET USER PASSWORD` “Administrator” “Password123”.
2. Stecken Sie das Flash-Laufwerk mit der Datei `reset_password.cfg` in den USB-Port des aktiven Onboard Administrator-Moduls ein. Die LED auf dem Onboard Administrator-Modul zeigt den aktiven OA an.
3. Navigieren Sie mittels Onboard Administrator Insight Display zum Hauptmenü, wählen Sie „USB Key Menu“ (USB-Schlüssel-Menü) aus und klicken Sie anschließend auf **OK**.
4. Wenn „Insight Display PIN Protection“ (Insight Display-PIN-Schutz) aktiviert ist, werden Sie zur Eingabe der PIN aufgefordert. Wählen Sie **Accept** (Übernehmen) aus, und klicken Sie auf **OK**.
5. Wählen Sie **Restore Configuration** (Konfiguration wiederherstellen) aus, und klicken Sie auf **OK**. Das USB-Flash-Laufwerk im Onboard Administrator-Modul wird geprüft, und die verfügbaren .cfg-Dateien werden aufgelistet.
6. Wählen Sie die Datei `reset_password.cfg` aus, und klicken Sie dann auf **OK**.

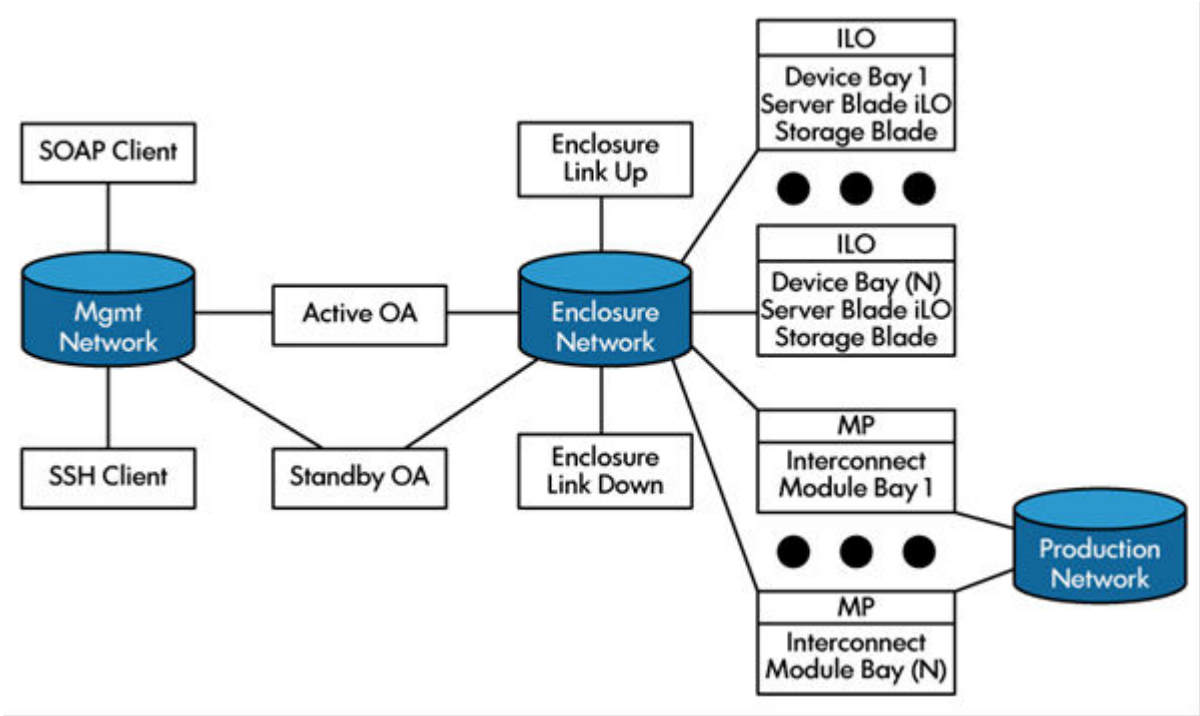
7. Wenn der Bildschirm „Confirm Operation“ (Vorgang bestätigen) angezeigt wird, klicken Sie auf **OK**.
8. Melden Sie sich mit der Benutzer-ID und dem Kennwort bei Onboard Administrator an, die in Schritt 1 angegeben wurden.

Sicherheitshinweise

Dieser Abschnitt beschreibt die Sicherheitsempfehlungen bezüglich der Architektur und der optimalen Vorgehensweise, die beim Konfigurieren von Onboard Administrator zu berücksichtigen sind, und vergleicht die Standardeinstellungen mit der vorherigen Version.

Übersicht über die BladeSystem-Netzwerkarchitektur

Alle Geräteeinschübe, Verbindungsmodule und Onboard Administrator-Module sind an ein internes Gehäuse-Netzwerk angeschlossen, das von einem aktiven Onboard Administrator-Modul verwaltet wird. Der Netzwerkdatenverkehr von Geschäftsanwendungen, die auf Server Blades ausgeführt werden, wird über die Verbindungsmodul-Switch-Module auf dem Produktionsnetzwerk weitergeleitet.



Obwohl eine Verbindung zwischen dem Management- und dem Produktionsnetzwerk möglich ist, sollte das Management-Netzwerk vom Produktionsdatenverkehr und dem Intranet isoliert werden. Im Hinblick auf die Sicherheit werden dadurch Zugriff und die Gefahr von Management-Schnittstellen-Attacken reduziert. Im Hinblick auf die Effizienz sorgen separate Netzwerke dafür, dass der Produktionsverkehr vom Management-Netzwerk ferngehalten wird.

Empfohlene optimale Vorgehensweisen bezüglich Sicherheit

Zusätzlich zu den optimalen Vorgehensweisen ist Folgendes zu beachten.

Physische Präsenz

Physischer Zugriff zu einem System geht oft mit Administratorberechtigungen einher. Der Onboard Administrator ist keine Ausnahme. Weitere Informationen zum Konfigurieren des Administratorzugriffs

auf Onboard Administrator finden Sie unter „Konfigurieren des HP BladeSystem c7000 Gehäuses und der Gehäusekomponenten“ („Konfigurieren von HP BladeSystem-Gehäusen und Gehäusekomponenten“ auf Seite 110).

- Überprüfen der physischen Verkabelung

  An dem BladeSystem-Gehäuse können viele Kabel angeschlossen sein. Die an die Verbindungsmodul-Switch-Module angeschlossenen Kabel sind im Allgemeinen für Produktionsnetzwerk-Datenverkehr vorgesehen. Alle anderen Kabel und Ports sind im Allgemeinen für den Datenverkehr des Gehäuse-Management-Netzwerks vorgesehen und sollten sorgfältig inspiziert werden.

  - Stellen Sie sicher, dass Gehäuse-Link-Ports nur mit Gehäuse-Link-Ports anderer Gehäuse verbunden sind.
  - Untersuchen Sie die seriellen Onboard Administrator-Ports auf unbefugte Verbindungen.
  - Untersuchen Sie die Onboard Administrator-USB-Ports auf unbefugte Verbindungen.

- Sichern des Insight Display-LCD-Bedienfeldes

  Das Insight Display-LCD-Bedienfeld ermöglicht die Konfiguration und Überwachung wichtiger Onboard Administrator-Einstellungen, z. B. die Konfiguration der Netzwerkadresse und das Ein-/Ausschalten von Server Blade-Einschüben, um nur einige kritische BladeSystem-Funktionen zu nennen. HP empfiehlt, das Insight Display-LCD-Bedienfeld insbesondere in einem Rechenzentrum mit mehreren Mietern durch eine PIN-Nummer zu schützen. Zudem schreiben bestimmte behördliche oder branchenspezifische Normen wie z. B. PCI möglicherweise vor, dass alle Schnittstellen durch eine PIN-Nummer bzw. ein Kennwort zu schützen sind, auch wenn sie keinen physischen Zugriff erfordern.

  Die Tasten des Insight Display-LCD-Bedienfelds sind im FIPS-Modus ON/DEBUG standardmäßig gesperrt. Weitere Informationen finden Sie unter „Registerkarte ‚FIPS‘“ (Registerkarte „FIPS“ auf Seite 140).

Festlegen der Werkseinstellungen vor der Hardware-Bereitstellung

Durch redundante Hardware soll sichergestellt werden, dass alle Einstellungen vorhanden sind, so dass das Onboard Administrator-Standby-Modul bei einem Ausfall des aktiven Onboard Administrator-Moduls die aktive Rolle übernehmen kann. Dies bedeutet, dass Informationen des lokalen Benutzerkontos auf dem Onboard Administrator-Standby-Modul dupliziert werden. Wenn „Enclosure IP Mode“ (Gehäuse-IP-Modus) konfiguriert ist, dann wird der private Schlüssel, der für die SSL-Kommunikation verwendet wird, auch auf dem Onboard Administrator-Standby-Modul gespeichert. (Der Gehäuse-IP-Modus ist standardmäßig nicht konfiguriert.) Je nach den Sicherheitsanforderungen für das Rechenzentrum sollten kritische Sicherheitsparameter in der Hardware gelöscht werden, bevor ein Gehäuse oder die Komponenten innerhalb des Gehäuses, wie Onboard Administrator, VC und iLO für HP BladeSystem außer Betrieb genommen oder erneut bereitgestellt werden.

Um sicherzustellen, dass alle kritischen Sicherheitsparameter gelöscht werden, stellen Sie die Werkseinstellungen mit SET FACTORY wieder her. Zudem kann das Administrator-Kennwort auf die Werkseinstellung „toe-tag“ eingestellt werden. Dazu kann das Kennwort manuell geändert oder ein serielles Kabel angeschlossen und das Verfahren für vergessene Kennwörter aufgerufen werden. Anweisungen finden Sie unter „Wiederherstellen des Administratorkennwortes“ (Wiederherstellen des Administratorkennworts auf Seite 15).

Isolieren des Management-Netzwerks

Ganz gleich wie sicher ein Gerät zu sein scheint, ist es immer wieder mit neuen Attacken und Sicherheitsrisiken zu rechnen. HP rät als vorbeugende Maßnahme in Übereinstimmung mit den optimalen Vorgehensweisen der Branche sehr dazu, das Management-Netzwerk vom

Produktionsnetzwerk zu trennen. Außerdem sollte das Management-Netzwerk nicht auf dem offenen Internet oder in der Firewall-DMZ platziert werden, ohne zusätzliche Zugangsauthentifizierung wie z. B. einen VPN/Tunnel vorzuschreiben.

Netzwerkports

Weitere Informationen zu Ports finden Sie unter „Zugriffsanforderungen“ (Zugriffsanforderungen auf Seite 3).

Weitere Informationen zum Verwalten der HP Software über eine Firewall finden Sie im *Managing HP Servers Through Firewalls with Insight Management White Paper*. Dieses Dokument kann von der HP Insight Management-Informationsbibliothek (http://www.hp.com/go/docs) heruntergeladen werden.

Kryptographische Sicherheitsfunktionen und Standardeinstellungen

Ab Onboard Administrator Version 3.71 werden die kryptographischen Fähigkeiten von Onboard Administrator durch Hinzufügen eines neuen FIPS-Modus signifikant verbessert. Der FIPS-Modus macht ein Reihe von Anforderungen geltend, die signifikant von Nicht-FIPS-Einstellungen und früheren Versionen abweichen. Die Sicherheitsverbesserungen eliminieren schwache Algorithmen und folgen im Allgemeinen den FIPS 140-2-Leitlinien. Weitere Informationen finden Sie in der nachstehenden Tabelle. An die Tabelle schließt sich eine Liste unterstützter SSH-Verschlüsselungsmethoden, SSH-Schlüsselaustauschalgorithmen und SSH-Nachrichtenauthentifizierungscode-Algorithmen an.

Der OA-Administrator kann die Einstellungen des FIPS-Modus ändern und kryptographische Protokolle und Chiffren über die Registerkarte **Enclosure Settings (Gehäuseeinstellungen)>Network Access (Netzwerkzugriff)>FIPS** (Registerkarte „FIPS“ auf Seite 140) aktivieren bzw. deaktivieren.

HINWEIS: Wenn eine Version der Onboard Administrator-Firmware vor Version 3.71 mit aktiviertem starken Verschlüsselungsmodus ausgeführt wird, wird beim Aktualisieren der Firmware auf Version 3.71 oder höher möglicherweise ein Eintrag im Onboard Administrator-Systemprotokoll (Syslog) protokolliert, der besagt, dass Onboard Administrator im FIPS-Modus betrieben wird. Dieser Syslog-Eintrag (`FIPS: OA is operating in FIPS Mode On`) ist nicht korrekt und kann ignoriert werden.

FIPS-Modus-Einstellungen

	OA 3.71 FIPS-Modus OFF	OA 3.71 FIPS-Modus ON	OA 4.01–OA 4.02 FIPS-Modus OFF	OA 4.01–OA 4.02 FIPS-Modus ON	OA 4.11-OA 4.22 FIPS-Modus OFF	OA 4.11-OA 4.22 FIPS-Modus ON	OA 4.30–OA 4.40 FIPS-Modus OFF	OA 4.30–OA 4.40 FIPS-Modus ON
Allgemeine Sicherheitselemente								
CSPs Zeroization (Nullierung kritischer Sicherheitsparameter)	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
Known Answer Tests (KATs)	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA

	OA 3.71 FIPS-Modus OFF	OA 3.71 FIPS-Modus ON	OA 4.01–OA 4.02 FIPS-Modus OFF	OA 4.01–OA 4.02 FIPS-Modus ON	OA 4.11-OA 4.22 FIPS-Modus OFF	OA 4.11-OA 4.22 FIPS-Modus ON	OA 4.30–OA 4.40 FIPS-Modus OFF	OA 4.30–OA 4.40 FIPS-Modus ON
Einschalttests	NEIN	JA	NEIN	JA	JA	JA	JA	JA
Fortlaufende PRNG-Tests	NEIN	JA	NEIN	JA	JA	JA	JA	JA
Mindestkennwortlänge erforderlich	3	8	3	8	3	8	3	8
Kennwortkomplexität erforderlich (Groß- und Kleinbuchstaben, Symbole)	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
FIPS-kompatibler PRNG (X9.31)	JA	JA	JA	JA	JA	JA	JA	JA
Telnet-Dienst deaktiviert	JA[1]	JA	NEIN[1]	JA	JA[1]	JA	JA[1]	JA[1]
„Enclosure IP Mode“ (Gehäuse-IP-Modus) deaktiviert	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
„Support Dump“ deaktiviert	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
SNMPv1- und SNMPv2-Services deaktiviert	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
Partitionsintegritäts-Prüfung	JA	JA	JA	JA	JA	JA	JA	JA
Erfordert Insight Display-LCD-PIN	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
SSL-Verschlüsselung								
SSL-Standardsc	2048 Bit	2048 Bit	2048 Bit	2048 Bit	2048 Bit	2048 Bit	2048 Bit	2048 Bit

	OA 3.71 FIPS-Modus OFF	OA 3.71 FIPS-Modus ON	OA 4.01–OA 4.02 FIPS-Modus OFF	OA 4.01–OA 4.02 FIPS-Modus ON	OA 4.11-OA 4.22 FIPS-Modus OFF	OA 4.11-OA 4.22 FIPS-Modus ON	OA 4.30–OA 4.40 FIPS-Modus OFF	OA 4.30–OA 4.40 FIPS-Modus ON
hlüsselgröße								
Hash-Signatur-Algorithmus für selbstsigniertes Standardzertifikat	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256	SHA256
Konfigurierbare SSL-Hash-Signatur-Algorithmen auf selbstsigniertem Zertifikat	JA	JA	JA	JA	JA	JA	JA	JA
SSL/TLS-Protokolle	SSLv3 TLSv1	TLSv1	SSLv3 TLSv1	TLSv1	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2
Zertifikate mit anderen Algorithmen als dem FIPS-Hash-Signatur-Algorithmus ablehnen[2]	NEIN	JA	NEIN	JA	NEIN	JA	NEIN	JA
Zulässige Zertifikatsig-natur-Hash-Algorithmen	md5, sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	md5, sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512	sha1, sha224, sha256, sha384, sha512
DES	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
CAST5	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
Blowfish	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
ARC4	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
3DES	JA	JA	JA	JA	JA	JA	JA	JA
AES 128-SHA	JA	JA	JA	JA	JA	JA	JA	JA

	OA 3.71 FIPS-Modus OFF	OA 3.71 FIPS-Modus ON	OA 4.01–OA 4.02 FIPS-Modus OFF	OA 4.01–OA 4.02 FIPS-Modus ON	OA 4.11-OA 4.22 FIPS-Modus OFF	OA 4.11-OA 4.22 FIPS-Modus ON	OA 4.30–OA 4.40 FIPS-Modus OFF	OA 4.30–OA 4.40 FIPS-Modus ON
DHE-RSA-AES256-SHA	JA	JA	JA	JA	JA	JA	JA	JA
AES256-SHA	JA	JA	JA	JA	JA	JA	JA	JA
DHE-RSA-AES128-SHA	JA	JA	JA	JA	JA	JA	JA	JA
EDH-RSA-DES-CBC3-SHA	JA	JA	JA	JA	JA	JA	JA	JA
DES-CBC3-SHA	JA	JA	JA	JA	JA	JA	JA	JA
ECDHE-RSA-DES-CBC3-SHA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
ECDHE-RSA-AES128-SHA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
ECDHE-RSA-AES256-SHA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
AES128-GCM-SHA256	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
AES256-GCM-SHA384	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
ECDHE-RSA-AES128-SHA256	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
AES128-SHA256	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
AES256-SHA256	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	JA
SSH-Schnittstelle								
Standardtyp und -größe des SSH-Schlüssels	DSA 2048	DSA 1024	DSA 2048	DSA 1024	RSA 2048	RSA 2048	RSA 2048	RSA 2048

	OA 3.71 FIPS-Modus OFF	OA 3.71 FIPS-Modus ON	OA 4.01–OA 4.02 FIPS-Modus OFF	OA 4.01–OA 4.02 FIPS-Modus ON	OA 4.11-OA 4.22 FIPS-Modus OFF	OA 4.11-OA 4.22 FIPS-Modus ON	OA 4.30–OA 4.40 FIPS-Modus OFF	OA 4.30–OA 4.40 FIPS-Modus ON
HMAC-MD5	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
HMAC-SHA1-96	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
HMAC-SHA1	JA	JA	JA	JA	JA	JA	JA	JA
HMAC-SHA256	NEIN	NEIN	NEIN	NEIN	JA	JA	JA	JA
HMAC-SHA512	NEIN	NEIN	NEIN	NEIN	JA	JA	JA	JA
Insight Display KVM								
RC4-Verschlüsselung	JA	NEIN	JA	NEIN	JA	NEIN	JA	NEIN
AES-Unterstützung für LCD KVM	JA	JA	JA	NEIN	JA	JA	JA	JA

[1] Telnet ist in Onboard Administrator 3.70 und höher standardmäßig deaktiviert. Im FIPS-Modus kann Telnet nicht aktiviert werden.
[2] Hash-Algorithmus für Standardzertifikat wurde bei Onboard Administrator 3.70 von SHA1 in SHA256 geändert. Sie können im Befehl `GENERATE KEY` verschiedene Schlüsselgrößen und Hash-Algorithmen auswählen.

Onboard Administrator 4.40 ändert den Anzeigenamen unterstützter TLS-Chiffren und führt eine strenge Reihenfolge ein, der aktivierte TLS Chiffren folgen müssen. Die Liste der unterstützten TLS-Chiffren und deren Reihenfolge werden in der folgenden Tabelle angegeben.

TLS Cipher Suites	OA 4.40 FIPS-Modus AUS	OA 4.40 FIPS-Modus EIN
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	JA	JA
TLS_RSA_WITH_AES_128_CBC_SHA	JA	JA
TLS_RSA_WITH_AES_256_CBC_SHA	JA	JA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	JA	JA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	JA	JA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	JA	NEIN
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	JA	NEIN
TLS_RSA_WITH_AES_128_GCM_SHA256	JA	JA
TLS_RSA_WITH_AES_256_GCM_SHA384	JA	JA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	JA	JA

TLS Cipher Suites	OA 4.40 FIPS-Modus AUS	OA 4.40 FIPS-Modus EIN
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	JA	JA
TLS_RSA_WITH_AES_128_CBC_SHA256	JA	JA
TLS_RSA_WITH_AES_256_CBC_SHA256	JA	JA

SSH-Verschlüsselungsmethoden

Für FIPS-Modus ON und FIPS-Modus OFF und für Onboard Administrator 3.71, 4.01 – 4.02, 4.11 – 4.22 und 4.30 – 4.40 werden die gleichen SSH-Verschlüsselungsmethoden unterstützt:

- `aes128-ctr`
- `aes192-ctr`
- `aes256-ctr`
- `aes128-cbc`
- `3des-cbc`
- `aes192-cbc`
- `aes256-cbc`
- `rijndael-cbc@lysator.liu.se`

SSH-Schlüsselaustauschalgorithmen

- OA 4.30 – 4.40

  ```
  ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
  ```

- OA 4.11 – 4.22

  ```
  diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
  ```

- OA 4.01 – 4.02

  ```
  diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
  ```

- OA 3.71

  ```
  diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
  ```

  - OA 4.01 und höhere Versionen besitzen eine Option zum Aktivieren/Deaktivieren von `diffie-hellman-group1-sha1`.
  - Der OA 4.01- und 4.02-Standard für `diffie-hellman-group1-sha1` ist deaktiviert.
  - Für OA 4.11 – 4.22 und 4.30 – 4.40 ist `diffie-hellman-group1-sha1` im FIPS-Modus OFF standardmäßig aktiviert und im FIPS-Modus ON standardmäßig deaktiviert.

SSH-Nachrichtenauthentifizierungscode-Algorithmen

Der unterstützte SSH-Nachrichtenauthentifizierungscode ist für FIPS-Modus EIN und FIPS-Modus AUS gleich. Onboard Administrator 3.70 und höher unterstützt für die SSH2-Nachrichtenauthentifizierung nicht mehr HMAC-MD5 und HMAC-SHA-96.

- OA 4.11 – 4.22 und 4.30 – 4.40

  `hmac-sha2-256`

  `hmac-sha2-512`

  `hmac-sha1`
- OA 4.01 – 4.02

  `hmac-sha1`
- OA 3.71

  `hmac-sha1`

2 HP BladeSystem c3000/c7000-Gehäuse – Hardwareinstallation

Installieren von Onboard Administrator-Modulen

Das HP BladeSystem c3000- und HP BladeSystem c7000-Gehäuse wird mit einem HP BladeSystem Onboard Administrator-Modul installiert und kann bis zu zwei Onboard Administrator-Module unterstützen. Installieren Sie die Onboard Administrator-Module unter Berücksichtigung der insgesamt bestellten Anzahl:

- Ein Onboard Administrator-Modul: Einschub 1
- Zwei Onboard Administrator-Module: Einschübe 1 und 2

Setzen Sie eine Onboard Administrator-Leerblende in den unbenutzten Onboard Administrator-Einschub ein.

HINWEIS: Wenn zwei Onboard Administrator-Module installiert wurden, ist das Modul in Einschub 1 aktiv und das Modul in Einschub 2 redundant.

Anweisungen zur Installation eines Onboard Administrator-Moduls finden Sie in den folgenden Dokumenten, die über die HP BladeSystem-Informationsbibliothek (http://www.hp.com/support/BladeSystem/docs) zugänglich sind:

- *HP BladeSystem c3000-Gehäuse Setup- und Installationshandbuch*
- *HP BladeSystem c7000-Gehäuse Setup- und Installationshandbuch*

HP BladeSystem Onboard Administrator-Verkabelung

Anleitungen zur Verkabelung eines Onboard Administrator-Moduls sind in den folgenden Dokumenten verfügbar, die über die HP BladeSystem-Informationsbibliothek (http://www.hp.com/support/BladeSystem/docs) zugänglich sind:

- HP BladeSystem c3000-Gehäuse Setup- und Installationshandbuch
- HP BladeSystem c7000-Gehäuse Setup- und Installationshandbuch

Wenn der Onboard Administrator-Verwaltungs-Ethernet-Port an ein Verwaltungs-LAN angeschlossen wird, über das auch Verbindungen zu Server-Ports hergestellt werden, dann stellen Sie sicher, dass die Server-Anwendungen den Onboard Administrator-Verwaltungsport nicht mit Broadcast-Paketen überlasten. Der Onboard Administrator-Verwaltungsport leitet alle Broadcast-Pakete vom Management-Netzwerk an alle Geräte innerhalb des Gehäuses weiter. Onboard Administrator zeichnet Netzwerkpaket-Überflutungsmeldungen im Systemprotokoll (syslog) des aktiven Onboard Administrator-Moduls auf, wenn eine hohe Rate von Paketen ermittelt wird. Wenn sich die Serververbindungen auf 1 GB und die Onboard Administrator-Verbindung auf 100 MB belaufen, kann der Port auf dem an den Onboard Administrator angeschlossenen Netzwerk-Switch leicht überwältigt werden. Bei Fortbestehen der Netzwerkpaket-Überflutung wird die Leistung des Onboard Administrators beeinträchtigt. Wenn die Kapazität des Onboard Administrators durch eine Paketüberflutung überwältigt wird, wird Onboard Administrator möglicherweise neu gestartet. Dieser Zustand tritt ein, da Onboard Administrator alle Pakete vom Netzwerk, an das er angeschlossen ist, inspizieren muss. Onboard Administrator kann somit als Verwaltungs-Verbindungsstelle für interne

Gehäusegeräte wie z. B. iIOs oder Virtual Connect-Verwaltungsschnittstellen fungieren. Ein Neustart von Onboard Administrator verursacht zwar keinen direkten Ausfall des Kundendatenverkehrs, kann aber insbesondere bei Konfigurationen mit Virtual Connect unnötige Unannehmlichkeiten bereiten.

Wenn der Onboard Administrator beim Einschalten des Gehäuses mit einem Netzwerk mit einem DHCP-Server verbunden wird, ist für den Onboard Administrator und jedes iLO (eines pro Blade) jeweils ein DHCP-Lease erforderlich.

Onboard Administrator-Ports

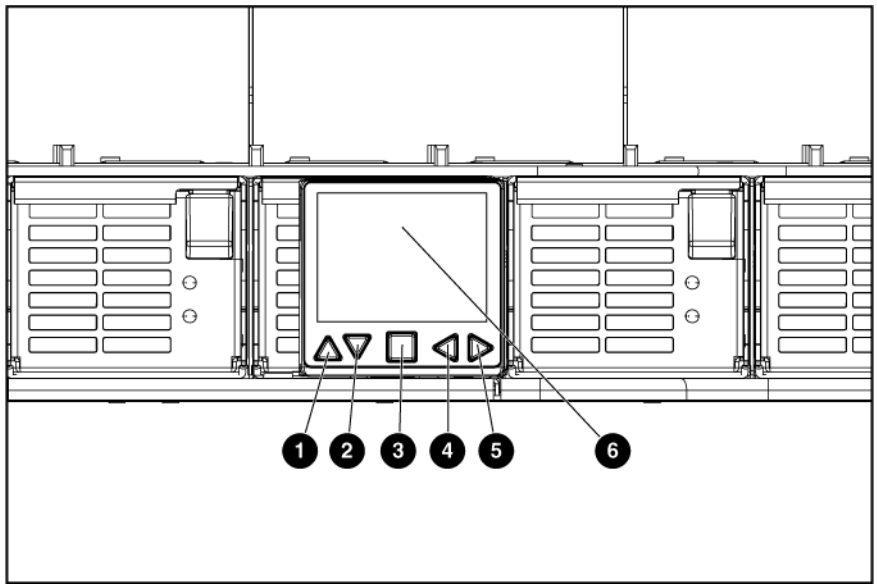
Die folgende Tabelle beschreibt die Ports am Onboard Administrator-Modul.

Porttyp	Beschreibung	Verwendungsrichtlinien
OA/ILO	Ethernet 1000BaseT RJ45-Anschluss	• Bietet Ethernet-Zugang zu OA und iLO auf jedem Blade. • Unterstützt zudem Verbindungsmodule mit Managementprozessoren, die zur Verwendung des Gehäuse-Verwaltungsnetzwerks konfiguriert sind. • Handelt automatisch 1000/100/10 aus oder kann so konfiguriert werden, dass 100 Mb oder 10 Mb Vollduplex erzwungen werden.
USB	USB 2.0-Anschluss Typ A	Für den Anschluss von USB-Geräten wie z. B. DVD-Laufwerke, USB-Schlüssellaufwerke oder eine Tastatur oder Maus zur KVM-Verwendung des Gehäuses. OA unterstützt USB-Geräte mit 4 GB oder weniger.
Serieller Anschluss	Serieller RS232 DB-9-Anschluss mit PC-Standard-Kontaktbelegung.	Bietet mit einem seriellen Nullmodem-Kabel direkten Zugriff auf das OA-Modul. Stellt einen direktionalen Kommunikationskanal zur Verfügung. • Dies ist hilfreich, wenn das OA-Modul im Netzwerk nicht zu erreichen ist. • Schließen Sie einen Computer an die OA-Befehlszeilenschnittstelle (CLI) an. Der bidirektionale Kommunikationskanal ermöglicht Benutzern beispielsweise, diagnostische Befehle auszuführen oder Informationen zum Gehäusestatus anzuzeigen. • Der Zugriff auf das OA-Modul ist ohne Anmeldeinformationen oder Kenntnis der IP-Adresse möglich. Sollten Sie Ihre OA-Administrator-Anmeldedaten vergessen haben, können Sie über den seriellen Port eine Verbindung mit dem OA aufbauen und das Kennwort zurücksetzen (siehe „Wiederherstellen des Administratorkennworts“ (Wiederherstellen des Administratorkennworts auf Seite 15)).
VGA-Anschluss	VGA DB-15-Anschluss mit PC-Standard-Kontaktbelegung. Die VGA-Ports des c3000-Gehäuses befinden sich an einem separaten Modul (dem KVM-Modul) auf der Rückseite des Gehäuses.	Ähnlich wie der serielle Port bieten sie zusätzlichen Zugriff auf das Rack-KVM und das Server Blades-iLO. Dieser Zugriff ermöglicht jedoch nur eine Anzeige von Daten. Über die KVM-Verbindung ist keine OA-Diagnose möglich. Schließen Sie zum Zugriff auf das Gehäuse-KVM-Menü einen Rack-KVM-Monitor an. Schließen Sie zum Zugriff auf die OA-CLI einen VGA-Monitor an.
Gehäuse-Link-down-Port	Stellt mit einem CAT5-Patch-Kabel eine Verbindung zum Gehäuse-	Dieser Port dient zum Anschluss verschiedener Gehäuse und zum Erstellen eines Clusters von Gehäusen. Wenn Gehäuse miteinander verbunden werden, muss zum Zugriff auf die

Porttyp	Beschreibung	Verwendungsrichtlinien
	Link-up-Port am Gehäuse unten her.	Gehäusegruppe nur die IP-Adresse des Basisgehäuses bekannt sein.
Gehäuse-Link-up-Port und Service-Port	Stellt mit einem CAT5-Patch-Kabel eine Verbindung zum Gehäuse-Link-down-Port am übergeordneten Gehäuse her.	Die gleiche Verwendung wie der Gehäuse-Link-down-Port. An einem Standalone-Gehäuse oder am obersten Gehäuse in einer Reihe von verbundenen Gehäusen fungiert der oberste Gehäuse-Link-up-Port als Service-Port.

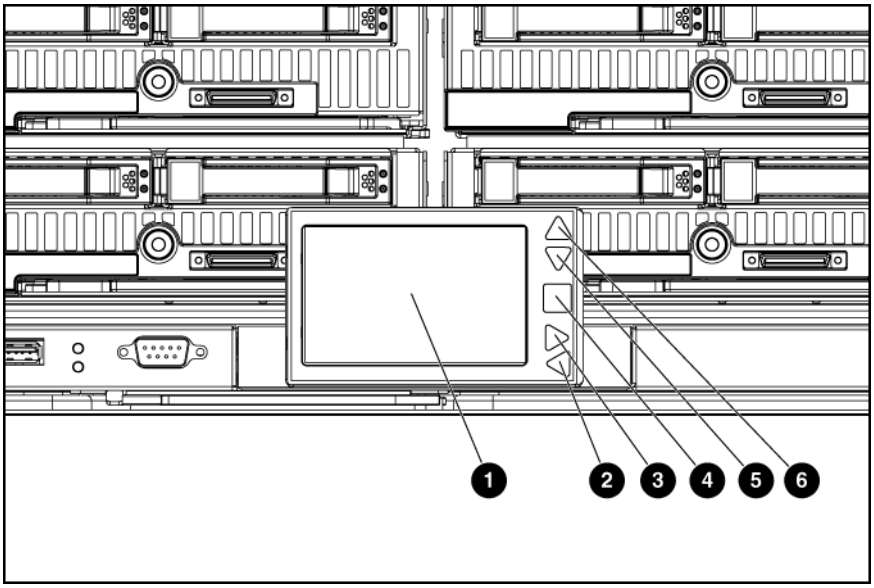
3 HP BladeSystem Insight Display

HP BladeSystem c7000 2-Zoll Insight Display-Komponenten



Element	Beschreibung	Funktion
1	Aufwärtspfeil-Taste	Verschiebt die Menüauswahl um eine Position nach oben.
2	Abwärtspfeil-Taste	Verschiebt die Menüauswahl um eine Position nach unten.
3	Taste „OK“	Übernimmt die markierte Auswahl und wechselt zum ausgewählten Menü.
4	Linkspfeil-Taste	Verschiebt die Menü- oder Navigationsleistenauswahl um eine Position nach links.
5	Rechtspfeil-Taste	Verschiebt die Menü- oder Navigationsleistenauswahl um eine Position nach rechts.
6	Insight Display-Bildschirm	Zeigt Hauptmenü-Fehlermeldungen und -Anweisungen an.

HP BladeSystem c3000 und c7000 3-Zoll Insight Display-Komponenten



Element	Beschreibung	Funktion
1	Insight Display-Bildschirm	Zeigt Hauptmenü-Fehlermeldungen und -Anweisungen an.
2	Linkspfeil-Taste	Verschiebt die Menü- oder Navigationsleistenauswahl um eine Position nach links.
3	Rechtspfeil-Taste	Verschiebt die Menü- oder Navigationsleistenauswahl um eine Position nach rechts.
4	Taste „OK“	Übernimmt die markierte Auswahl und wechselt zum ausgewählten Menü.
5	Abwärtspfeil-Taste	Verschiebt die Menüauswahl um eine Position nach unten.
6	Aufwärtspfeil-Taste	Verschiebt die Menüauswahl um eine Position nach oben.

Insight Display – Übersicht

Mithilfe des Insight Displays kann der Rack-Techniker die Erstkonfiguration des Gehäuses vornehmen. Darüber hinaus liefert das Insight Display Informationen zum Zustand und Betrieb des Gehäuses. Die Farbe des Insight Displays variiert je nach Zustand des Gehäuses:

- Blau – Das Insight Display leuchtet blau, wenn die Gehäuse-UID aktiv ist. Die Gehäuse-UID wird automatisch aktiviert, wenn das Gehäuse zum ersten Mal eingeschaltet wird. Sie kann über die Option „Turn Enclosure UID On“ (Gehäuse-UID aktivieren) im Hauptmenü oder durch Drücken der Gehäuse-UID-Taste am Management-Interposer aktiviert werden.

  Wenn die Gehäuse-UID aktiv ist, beginnt das Insight Display nach zwei Minuten Inaktivität zu blinken. Drücken Sie eine beliebige Taste auf dem Insight Display, um die Blinkanzeige zu beenden und den Bildschirm zu reaktivieren.

- Grün – Das Insight Display leuchtet grün, wenn kein Fehler- oder Alarmzustand vorliegt und der Gehäusebetrieb normal ist. Nach zwei Minuten Inaktivität erlischt die Insight Display-Anzeige. Drücken Sie eine beliebige Taste auf dem Insight Display, um den Bildschirm zu reaktivieren.

- Gelb – Das Insight Display leuchtet gelb, wenn der Onboard Administrator einen Fehler- oder Alarmzustand erkennt. Auf dem Bildschirm werden Informationen zum betreffenden Zustand angezeigt.

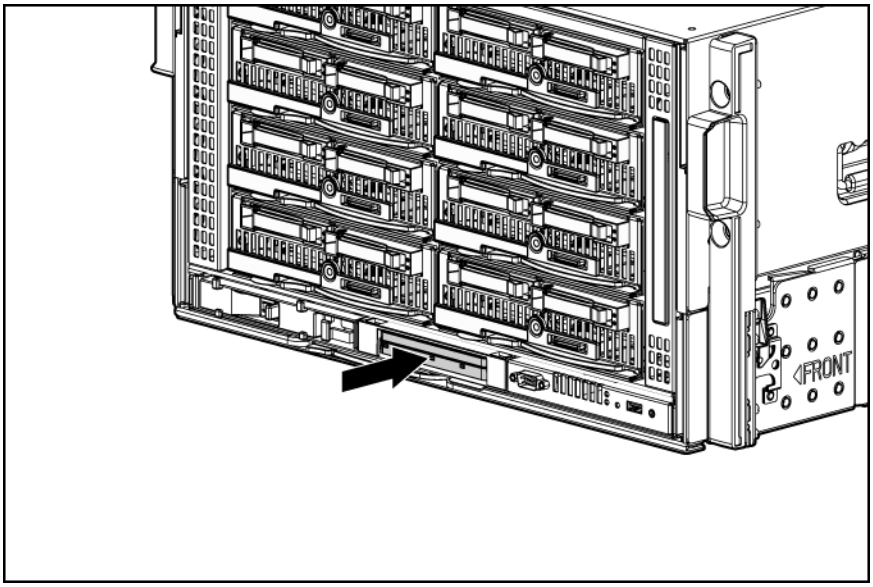
  Nach zwei Minuten Inaktivität blinkt das Insight Display gelb und zeigt damit einen Fehler- oder Alarmzustand an. Wenn die Gehäuse-UID aktiv ist und ein Fehler- oder Alarmzustand vorliegt, leuchtet das Insight Display blau, da die Gehäuse-UID eine höhere Priorität als der Alarm besitzt. Drücken Sie eine beliebige Taste auf dem Insight Display, um den Bildschirm zu reaktivieren.

- Dunkel (keine Stromversorgung) – Das Insight Display befindet sich in einer Phase zweiminütiger Inaktivität. Wenn keine Aktion stattfindet und auch kein Alarmzustand vorliegt, schaltet sich die Bildschirmanzeige nach zwei Minuten aus. Drücken Sie eine beliebige Taste auf dem Insight Display, um den Bildschirm zu reaktivieren.

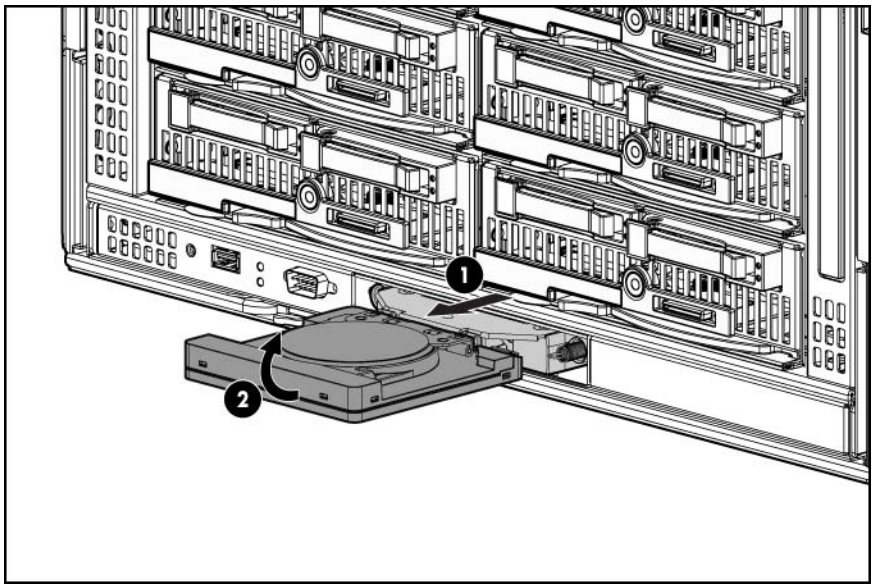
Das Symbol für den Gehäusezustand befindet sich in jedem Bildschirm unten links und gibt den Zustand des Gehäuses an. Platzieren Sie den Cursor auf dem Symbol für den Gehäusezustand, und rufen Sie mit „OK“ den Bildschirm „Health Summary“ (Zustand – Zusammenfassung) aus einem beliebigen Bildschirm von Insight Display heraus auf.

Zugreifen auf das HP BladeSystem c3000 Insight Display

1. Um auf das Insight Display zuzugreifen, drücken Sie auf das freiliegende Ende.



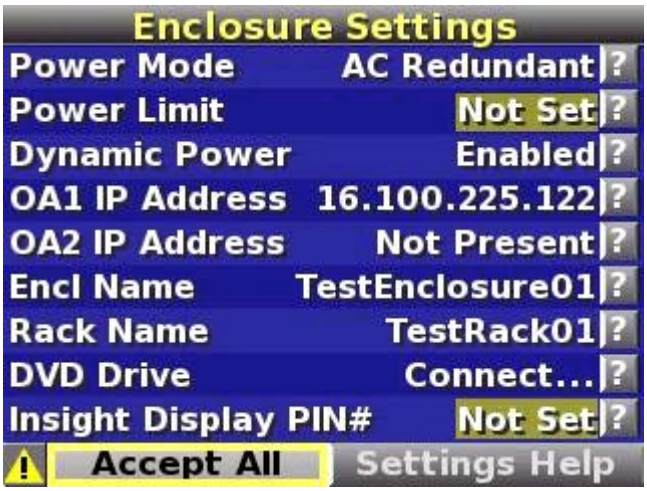
2. Ziehen Sie das Insight Display aus dem Gehäuse, bis es einrastet, und kippen Sie es nach oben.



Durchführen der Insight Display-Installation

Zur Identifizierung des Gehäuses leuchten die Gehäuse-UID-Anzeige auf der Rückseite und der Hintergrund des Insight Displays blau, wenn das Gehäuse zum ersten Mal eingeschaltet wird. Wenn das Gehäuse zum ersten Mal eingeschaltet wird, startet das Insight Display einen Installationsassistenten, der Sie durch den Konfigurationsprozess führt. Zu Anfang der Installation schaltet der Assistent automatisch die Gehäuse-UID ein. Nach Abschluss der Installation schaltet der Assistent die Gehäuse-UID aus. Nach der Konfiguration des Gehäuses überprüft das Insight Display, ob eventuell Installations- oder Konfigurationsfehler vorliegen. Liegen Fehler vor, leitet Sie das Insight Display bei durch das Verfahren, mit dem sich die Fehler beheben lassen.

Als erster Bildschirm wird „Enclosure Settings“ (Gehäuseeinstellungen) angezeigt.


Enclosure Settings
Power Mode AC Redundant ?
Power Limit Not Set ?
Dynamic Power Enabled ?
OA1 IP Address 16.100.225.122 ?
OA2 IP Address Not Present ?
Encl Name TestEnclosure01 ?
Rack Name TestRack01 ?
DVD Drive Connect... ?
Insight Display PIN# Not Set ?
Accept All
Settings Help

1. Überprüfen Sie jede Einstellung auf dem Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) (siehe Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) auf Seite 40) auf deren Richtigkeit.
2. Wenn Sie einen Wert ändern möchten, platzieren Sie den Cursor auf der Menüoption, die bearbeitet werden soll, und drücken Sie die Taste **OK**.
3. Nehmen Sie die notwendige Änderung vor, platzieren Sie den Cursor auf **Accept** (Übernehmen), und drücken Sie die Taste **OK**, um zum Menü „Enclosure Settings“ (Gehäuseeinstellungen) zurückzukehren. Wiederholen Sie diesen Schritt, bis alle Optionen im Menü „Enclosure Settings“ (Gehäuseeinstellungen) richtig sind.

TIPP: Wählen Sie das Symbol „?“ aus, um ausführliche Hilfeinformationen zu den einzelnen Einstellungen oder Themen aufzurufen.

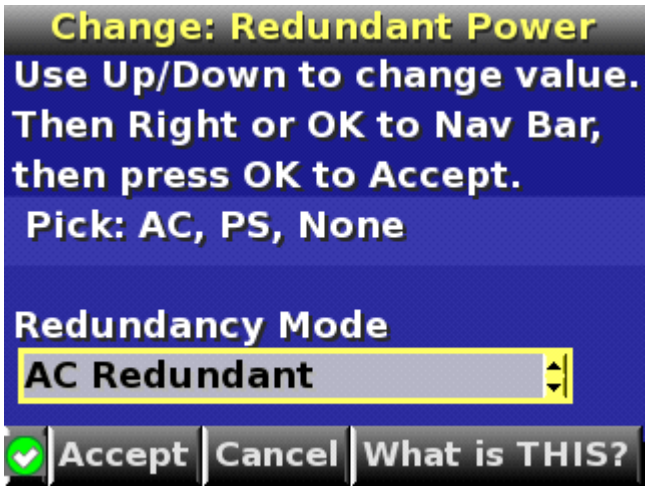
TIPP: Platzieren Sie den Cursor innerhalb einer beliebigen Menüoption auf der Schaltfläche **What is This** (Was ist das), und drücken Sie die Taste **OK** , um weitere Informationen zu den einzelnen Einstellungen, Optionen oder Alarmmeldungen anzuzeigen.

4. Wenn alle Einstellungen im Menü „Enclosure Settings“ (Gehäuseeinstellungen) richtig sind, platzieren Sie den Cursor auf der Schaltfläche **Accept All** (Alle übernehmen), und drücken Sie die Taste **OK**, um die aktuellen Einstellungen zu übernehmen.

   Sie können die folgenden Optionen im Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) ändern:

   Power Mode (Stromversorgungsmodus): Die Standardeinstellung ist „AC Redundant“ (Netzredundant). Die folgenden Optionen können ausgewählt werden:

   - AC Redundant (Netzredundant)
   - Power Supply Redundant (Netzteilredundant)
   - Keine



   Power Limit (Strombegrenzung): Die Standardeinstellung ist „Not Set“ (Nicht festgelegt). Sie können das Limit in Schritten von 50 Watt ändern.

ACHTUNG: Setzen Sie bei der Berechnung des Werts für die Option „Power Limit Watts AC“ (Strombegrenzung in Watt) nur 80 % der maximalen Leistung an, um das Auslösen des Leistungsschalters zu verhindern (nur USA).

ACHTUNG: Wenn der berechnete Spitzenleistungswert für Ihren Standort zu hoch ist, legen Sie den Wert für „Power Limit Watts AC“ (Strombegrenzung in Watt) so fest, dass er den Möglichkeiten Ihres Standortes entspricht.

Dynamic Power (Dynamische Stromversorgung): Die Standardeinstellung ist „Disabled“ (Deaktiviert). Die folgenden Optionen können ausgewählt werden:

- **Enabled** (Aktiviert): Einige der Netzteile können in den Standby-Betrieb geschaltet werden, um die Gesamteffizienz des Stromversorgungssubsystems des Gehäuses automatisch zu steigern.
- **Disabled** (Deaktiviert): Alle Netzteile teilen die Last. Die Effizienz des Stromversorgungssubsystems ist je nach Last unterschiedlich.

HINWEIS: Die Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus) wird bei allen c3000-Netzteilen unterstützt. Sie wird bei allen c7000-Netzteilen außer solchen unterstützt, die mit niedriger Eingangsspannung (Nennwert 100-120 VAC) betrieben werden.

OA1 IP Addr (OA1 IP-Adresse): Die Standardeinstellung ist „DHCP“. Wird keine IP-Adresse empfangen, lautet die IP-Adresse 0.0.0.0. In dieser Option werden IP-Adresse, Maske und Gateway festgelegt.

OA2 IP Addr (OA2-IP-Adresse): Ist dieses Modul vorhanden, ist die Standardeinstellung „DHCP“. Wird keine IP-Adresse empfangen, lautet die IP-Adresse 0.0.0.0. Wenn nur ein Onboard Administrator-Modul installiert ist, wird auf dem Bildschirm die Meldung „Not Present“ (Nicht vorhanden) angezeigt.

Enclosure Name (Gehäusename): Die Standardeinstellung ist ein eindeutiger, werksseitig vergebener Name. Die akzeptierten Werte sind 0–9, A–Z, a–z, -, _ und □. Durch das Symbol □ wird das Ende des Namens ausgewiesen.

HINWEIS: Verwenden Sie das Symbol □ nicht in der Mitte eines Textfelds. Die Einträge in Textfeldern werden bis zum letzten Zeichen vor dem Symbol □ abgeschnitten.

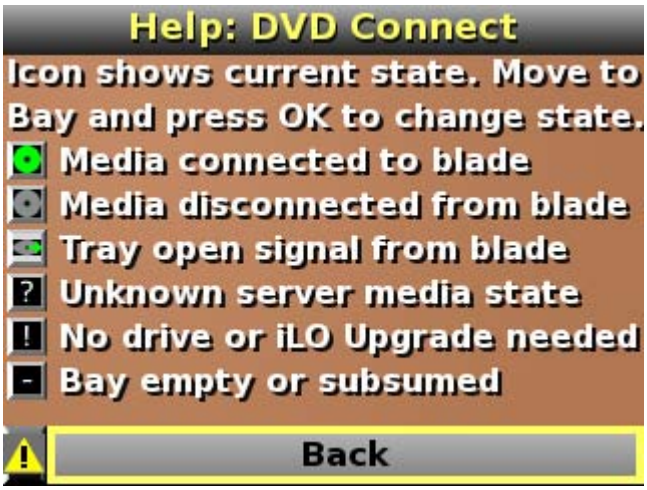
TIPP: Wählen Sie in der Navigationsleiste **Clear** (Löschen), um Einträge in Textfeldern bis zum Symbol □ zu löschen.

Rack Name (Rack-Name): Der Standardwert ist „UnnamedRack“ (UnbenanntesRack). Die akzeptierten Werte sind 0–9, A–Z, a–z, -, _ und □. Durch das Symbol □ wird das Ende des Namens ausgewiesen.

DVD Drive (DVD-Laufwerk): Die Standardeinstellung für alle Blades ist „Disconnected“ (Nicht verbunden). Das Menü „DVD Connect Status“ (DVD-Verbindungsstatus) zeigt den aktuellen DVD-Verbindungsstatus mit einem Symbol an.

Um zum Menü „Blade DVD Connection“ (Blade-DVD-Verbindung) zu navigieren, wählen Sie im Menü „DVD Connect“ (DVD-Verbindung) ein DVD-Symbol aus.

Um die verschiedenen DVD-Verbindungssymbole und deren Bedeutung anzuzeigen, klicken Sie auf „Help“ (Hilfe).


Help: DVD Connect
Icon shows current state. Move to
Bay and press OK to change state.
Media connected to blade
Media disconnected from blade
Tray open signal from blade
Unknown server media state
No drive or iLO Upgrade needed
Bay empty or subsumed
Back

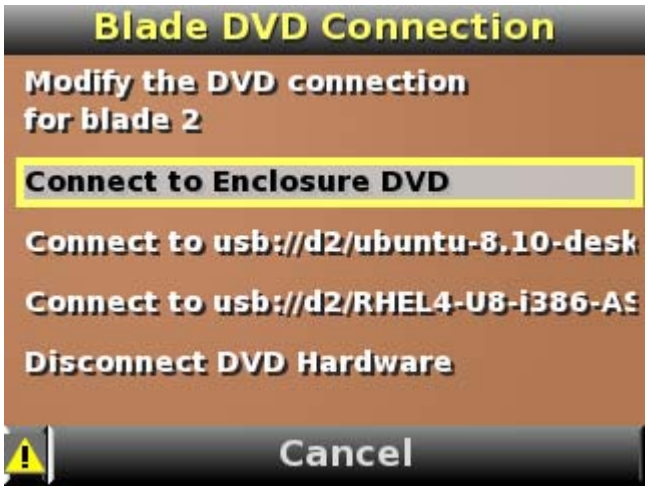
Wenn die „Insight Display PIN#“ (Insight Display-PIN-Nr.) festgelegt ist, ist das DVD-Laufwerksmenü durch die LCD-PIN geschützt. Um die Gehäuse-DVD-Einstellungen anzuzeigen oder zu ändern, müssen Sie an der LCD die richtige PIN eingeben.

Um einen Blade mit einer CD, DVD, oder ISO-Datei zu verbinden, navigieren Sie entweder zu einem einzelnen Server-DVD-Symbol oder zur Schaltfläche **All Blades** (Alle Blades), und drücken Sie **OK**.

Aus dem Menü „Blade DVD Connection“ (Blade-DVD-Verbindung) geht hervor, ob zum Herstellen einer Verbindung zu den ausgewählten Servern im Menü „DVD Connect Status“ (DVD-Verbindungsstatus) eine Gehäuse-DVD oder eine ISO-Datei auf einem USB-Schlüssel verfügbar ist. Wenn mehrere ISO-Dateien auf dem USB-Schlüssel zu finden sind, umfassen die Optionen möglicherweise mehrere Seiten. Um die nächste Seite mit Verbindungsoptionen anzuzeigen, wählen Sie die Schaltfläche **Next Page** (Nächste Seite).

- **Connect to** (Verbinden mit): Wählen Sie eine der derzeit verfügbaren Optionen aus, und klicken Sie auf **OK**, um die betreffende Option auszuwählen und das Menü **Connect: Blade DVD** (Blade-DVD verbinden) aufzurufen. In diesem Menü können Sie bestimmten, ob die Server mit diesen verbundenen Medien neu gestartet oder im bestehenden Stromversorgungszustand belassen werden sollen.

- **Disconnect DVD Hardware** (DVD-Hardware trennen): Trennt die aktuelle Medienverbindung und kehrt zu dem Menü **DVD Connect Status** (DVD-Verbindungsstatus) zurück.



Die folgenden Optionen können ausgewählt werden:

- **No Power Change** (Keine Stromversorgungsänderung): Verbindet die ausgewählten Medien nur mit dem Server.
- **Connect and Reboot** (Verbinden und Neustarten): Verbindet die ausgewählten Medien mit den ausgewählten Servern und startet die ausgewählten Server neu.

5. Um alle Einstellungen zu übernehmen und fortzufahren, navigieren Sie zu **Accept All** (Alle übernehmen) unten auf dem Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen), und drücken Sie die Taste **OK**.

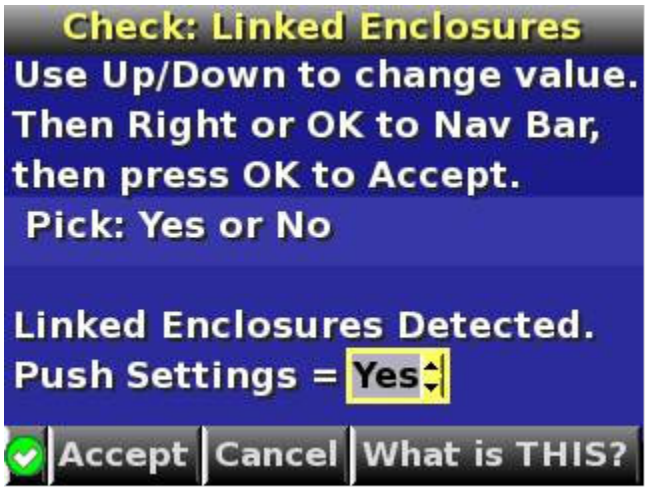
   Wenn das Onboard Administrator-Modul andere Gehäuse erkennt, wird die Meldung „Linked enclosures detected“ (Verbundene Gehäuse erkannt) angezeigt.

6. Verwenden Sie die Pfeile nach oben und nach unten, um die Option **Push Settings =** (Einstellungen weitergeben =) auf einen der folgenden Werte zu ändern:

   - **Yes** (Ja): Kopiert die konfigurierten Stromversorgungseinstellungen, den Rack-Namen und die LCD-Sperr-PIN (sofern festgelegt) vom Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) auf die erkannten Gehäuse.

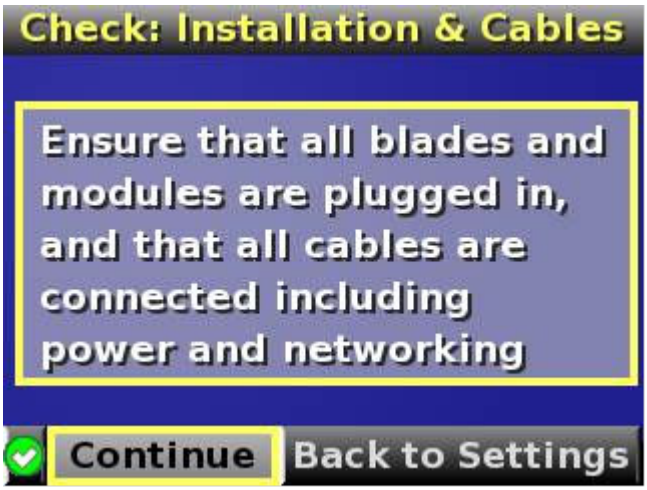
- **No** (Nein): Fährt nur mit der Konfiguration des aktuellen Gehäuses fort. Auf allen erkannten Gehäusen muss der Insight Display-Installationsassistent ausgeführt werden. Wählen Sie diese Option, wenn für jedes Gehäuse andere Stromversorgungseinstellungen erforderlich sind.

HINWEIS: Wenn Ihr Standort die statische IP-Adressierung für die Onboard-Administrator-Module verwendet, müssen Sie diese IP-Adressen für jedes Insight Display separat manuell in das Insight Display eintragen. Sie können diese IP-Adressen für die Onboard-Administrator-Module eingeben, bevor Sie die Einstellungen an die benachbarten Gehäuse senden. Nach Beendigung des Installationsassistenten können Sie zum Menü „Enclosure Settings“ (Gehäuseeinstellungen) zurückkehren, um die IP-Adressen der Onboard-Administrator-Module bei Bedarf zu ändern.



7. Platzieren Sie den Cursor auf **Accept** (Übernehmen), und drücken Sie die Taste **OK**.

   Der Installationsassistent zeigt den Bildschirm „Check: Installation and Cables“ (Prüfen: Installation und Kabel) an.

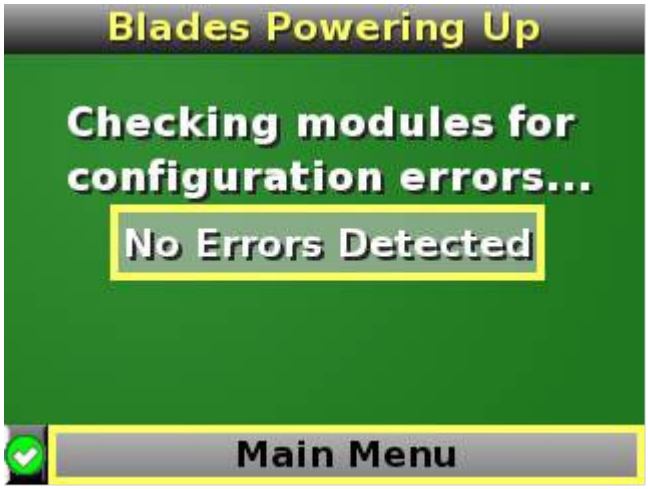

Check: Installation & Cables
Ensure that all blades and modules are plugged in, and that all cables are connected including power and networking
Continue
Back to Settings

8. Vergewissern Sie sich, dass alle Komponenten installiert und angeschlossen sind.
9. Um die Überprüfung auf Konfigurations-und Installationsfehler zu starten, wählen Sie **Continue** (Fortfahre) und klicken Sie auf **OK**. Bei Auswahl der Option **Continue** (Fortfahren) wird die Gehäuse-UID automatisch deaktiviert. Bei der Einstellung **Push Settings = Yes:** (Einstellungen weitergeben = Ja):

- Die Gehäuseeinstellungen werden an benachbarte Gehäuse weitergegeben.
- Die Installationsassistenten werden auf jedem benachbarten Gehäuse ausgeführt.
- Die Gehäuse-UID wird auf den benachbarten Gehäusen deaktiviert.

Wenn keine Fehler festgestellt wurden, wird die hintere Gehäuse-UID deaktiviert, und der Insight Display-Bildschirm leuchtet grün.

10. Um zum Hauptmenü zurückzukehren, drücken Sie **OK**. Die Einrichtung und Konfiguration von Gehäuse- und Blade-Hardware ist abgeschlossen.



HINWEIS: Wenn Fehler festgestellt wurden, leuchtet der Insight Display-Bildschirm gelb, und der Bildschirm „Health Summary“ (Zustand – Zusammenfassung) wird angezeigt. Weitere Informationen zur Behebung von Konfigurationsfehlern finden Sie unter „Insight Display-Fehlermeldungen“ (Insight Display-Fehlermeldungen auf Seite 47).

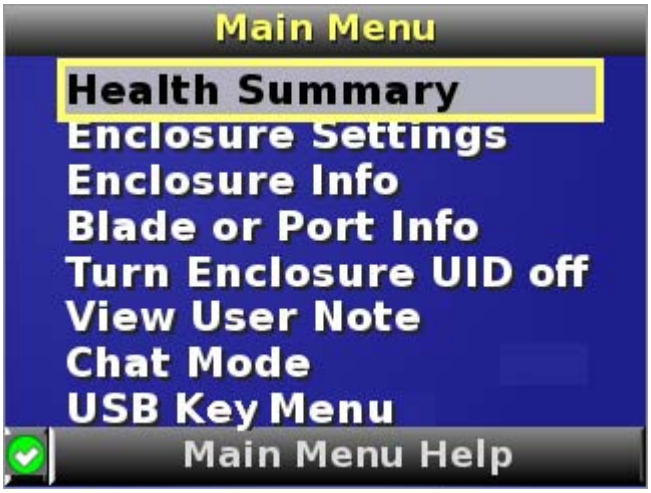
Konfigurationsfehler verhindern den Betrieb des Gehäuses und sollten sofort behoben werden.

11. Öffnen Sie einen Browser, und stellen Sie über die Onboard Administrator-IP-Adresse, die im Insight Display-Installationsassistenten konfiguriert wurde, eine Verbindung zum aktiven Onboard Administrator-Modul her.
12. Geben Sie den Benutzernamen und das Kennwort ein, die Sie zusammen mit dem Onboard Administrator-Modul erhalten haben, um auf die Remote-Weboberfläche des Onboard Administrators zuzugreifen und den Onboard Administrator-Assistenten für die erstmalige Installation durchzuführen.

Navigieren im Insight Display

Navigieren Sie mit den Pfeiltasten auf dem Bedienfeld des Insight Displays durch die Menüs und die Optionen.

Als erstes Menü wird „Main Menu“ (Hauptmenü) aufgerufen:

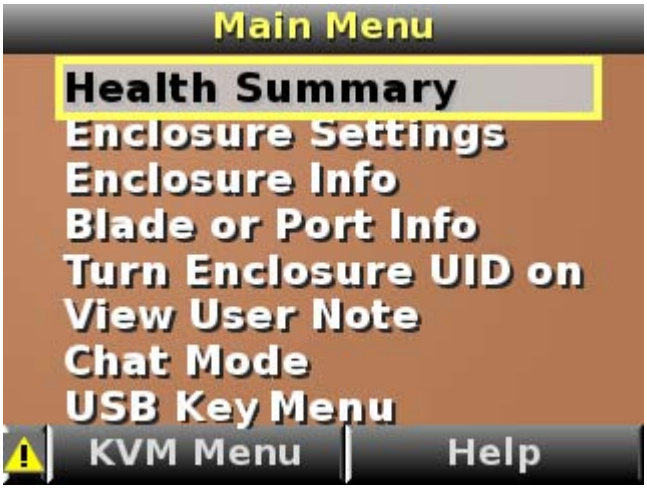


Das Hauptmenü des Insight Displays bietet die folgenden Menüoptionen:

- Health Summary (Zustand – Zusammenfassung)
- Enclosure Settings (Gehäuseeinstellungen)
- Enclosure Info (Gehäuse-Info)
- Blade Info (Blade-Info) oder Port Info (Port-Info)
- Turn Enclosure UID on/off (Gehäuse-UID aktivieren/deaktivieren)
- View User Note (Benutzernotiz anzeigen)
- Chat Mode (Chat-Modus)
- USB Key Menu (USB-Schlüssel-Menü)

Wenn das aktive Onboard Administrator-Modul die KVM-Funktion erkennt, wird eine KVM-Menüschaltfläche in der Navigationsleiste im Hauptmenü angezeigt. Mit Auswahl des KVM-Menüs wird das Insight Display gelöscht und die VGA-Verbindung von Onboard Administrator aktiviert.

Die KVM-Funktion ist in der folgenden Abbildung des Hauptmenüs sichtbar.



Ausführliche Informationen zum „Main Menu“ (Hauptmenü) des Insight Display finden Sie im *HP BladeSystem Insight Display Benutzerhandbuch*.

TIPP: Platzieren Sie den Cursor innerhalb einer beliebigen Menüoption auf der Schaltfläche **What is This** (Was ist das), und drücken Sie die Taste **OK** , um weitere Informationen zu den einzelnen Einstellungen, Optionen oder Alarmmeldungen anzuzeigen.

Mit den Optionen in der Navigationsleiste können Sie:

- Vor und zurück durch die Alarmbildschirme navigieren.
- Zum Hauptmenü zurückkehren.
- Änderungen der aktuellen Einstellungen übernehmen.
- Änderungen der aktuellen Einstellungen verwerfen.
- Über das Symbol „Health Summary“ (Zustand – Zusammenfassung) in der Navigationsleiste von jedem beliebigen Bildschirm aus auf den Bildschirm „Health Summary“ (Zustand – Zusammenfassung) zugreifen.

Bildschirm „Health Summary“ (Zustand – Zusammenfassung)

Der Bildschirm „Health Summary“ (Zustand – Zusammenfassung) zeigt den gegenwärtigen Zustand des Gehäuses an. Der Bildschirm „Health Summary“ (Zustand – Zusammenfassung) ist wie folgt erreichbar:

- durch Auswahl der Option **Health Summary** (Zustand – Zusammenfassung) im Hauptmenü.
- über das Symbol **Health Summary icon** (Zustand – Zusammenfassung) in einem beliebigen Insight Display-Bildschirm.

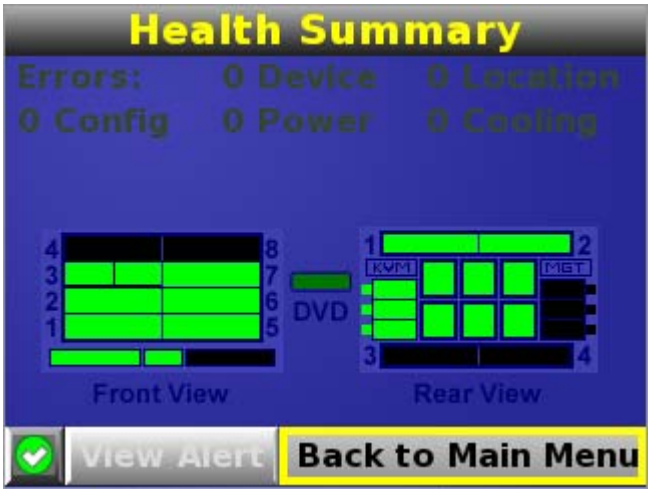
Wenn ein Fehler- oder Alarmzustand festgestellt wird, zeigt der Bildschirm „Health Summary“ (Zustand – Zusammenfassung) die Gesamtzahl der Fehlerbedingungen sowie die Fehlerpositionen an.

Wählen Sie in der Navigationsleiste die Option **Next Alert** (Nächste Alarmmeldung), und drücken Sie die Taste **OK**, um die einzelnen Fehlerbedingungen anzuzeigen. Das Insight Display zeigt jede Fehlerbedingung nach ihrem Schweregrad an. Kritische Alarmmeldungen werden zuerst angezeigt (sofern vorhanden). Danach folgen die Warnhinweise.

Wenn der Betrieb des Gehäuses normal ist, wird der Bildschirm „Health Summary“ (Zustand – Zusammenfassung) grün angezeigt. Die leuchtend grünen Rechtecke bezeichnen Komponenten, die installiert und eingeschaltet sind. Ein dunkelgrünes Rechteck steht für eine Komponente, die zwar installiert ist, jedoch ausgeschaltet wurde, ohne dass ein Fehler vorliegt. Ein schwarzes Rechteck steht für einen leeren Einschub.

Hinweis: Bei der c-Class-Gehäuse-DVD-Funktion bedeutet ein schwarzes DVD-Rechteck, dass kein DVD-Laufwerk am Onboard Administrator angeschlossen ist, während ein dunkelgraues Rechteck bedeutet, dass das DVD-Laufwerk vorhanden ist, aber keine Medien eingelegt sind. Ein dunkelgraues Rechteck bedeutet, dass Medien vorhanden sind, aber nicht aktiv mit einem Server verbunden sind, oder dass alle angeschlossenen Server einen Auswurfbefehl ausgegeben haben, so dass der Datenträger aus dem Laufwerk genommen werden kann. Ein hellgrünes Rechteck bedeutet, dass Medien im Laufwerk vorhanden sind und aktiv mit mindestens einem Server im Gehäuse verbunden sind und dass das Laufwerksfach geschlossen ist.

Bei Auftreten eines Fehlers ändert sich die Hintergrundfarbe des Bildschirms „Health Summary“ (Zustand – Zusammenfassung) von grün in gelb. Der Fehler wird bei Warnungen durch gelbe Rechtecke und bei Fehlern durch rote Rechtecke hervorgehoben. Die Symbole für den allgemeinen Zustand des Gehäuses in der linken Ecke aller Insight Display-Bildschirme zeigen den allgemeinen Zustand des Gehäuses an.



Wählen Sie die Option **View Alert** (Alarmmeldung anzeigen), und drücken Sie die Taste „OK“, um die Fehler anzuzeigen.

Wählen Sie **Details**, um detaillierte Angaben zum Fehler anzuzeigen.

Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen)

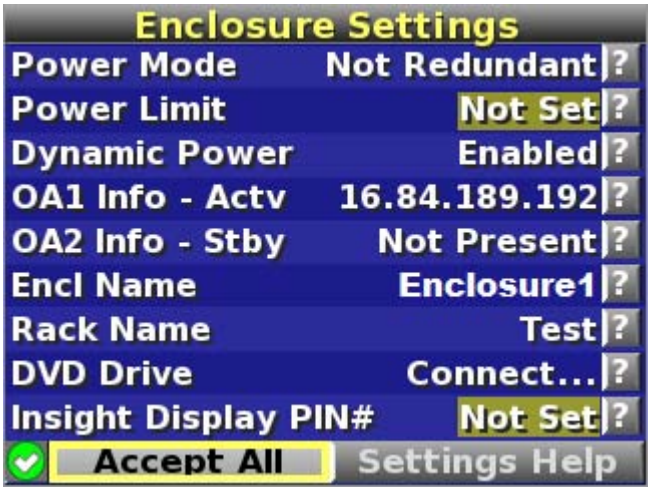
Der Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) zeigt die folgenden Einstellungsinformationen für das Gehäuse an:

- Einstellung für „Power Mode“ (Stromversorgungsmodus)
- Einstellung für „Power Limit“ (Strombegrenzung)
- Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus)
- Aktive und Standby-OA-IP-Adressen
- Enclosure Name (Gehäusename)
- Rack Name (Rack-Name)
- DVD Drive (CD/DVD-Laufwerk)
- Insight Display PIN

HINWEIS: Mit der Einstellung für das DVD-Laufwerk kann die Verbindung zwischen einer im optionalen c3000-Gehäuse-DVD-Laufwerk geladenen CD oder DVD und einem, mehreren oder allen Server Blades im Gehäuse hergestellt oder getrennt werden. Diese Funktion kann verwendet werden, um ein Betriebssystem oder Software auf Server Blades zu installieren. Wenn kein optionales DVD-Laufwerk vorhanden ist, kann stattdessen ein externes HP USB-DVD-Laufwerk mit dieser Funktion verwendet werden.

TIPP: Legen Sie eine PIN-Nummer fest, um die Gehäuseeinstellungen vor unbefugten Änderungen zu schützen.

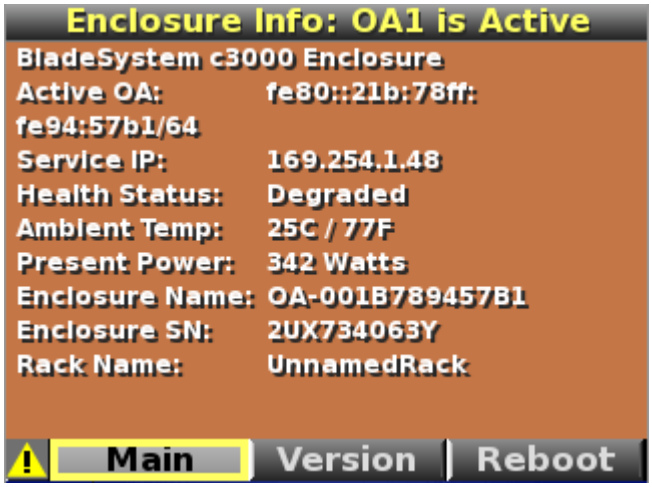
Platzieren Sie den Cursor auf einer Einstellung oder dem Fragezeichen (?), und drücken Sie die Taste OK, um die Einstellung zum Ändern oder Hilfeinformationen zu dieser Einstellung anzuzeigen.



Bildschirm „Enclosure Info“ (Gehäuse-Info)

Der Bildschirm „Enclosure Info“ (Gehäuse-Info) zeigt die folgenden Informationen für das Gehäuse an:

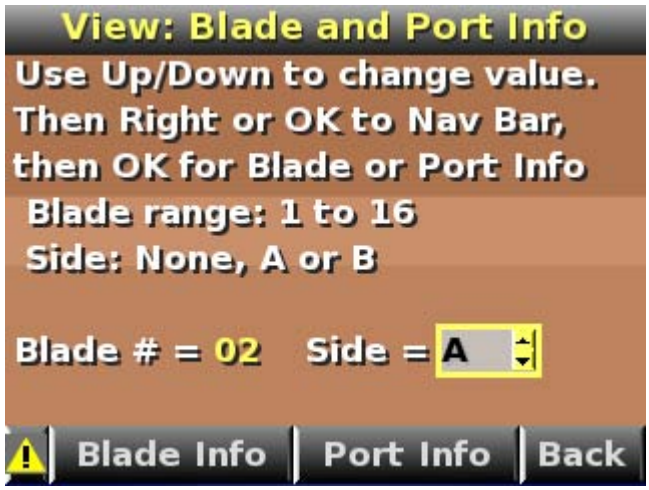
- Die aktive OA-IP-Adresse „OA Active IP“
- Die aktive OA-Service-IP-Adresse „OA Service IP“
- Current health status (Aktueller Zustand)
- Current ambient temperature (Aktuelle Umgebungstemperatur)
- Current AC input power (Aktueller Eingangsstrom)
- Name
- Serial Number (Seriennummer)
- Rack Name (Rack-Name)



Bildschirm „Blade or Port Info“ (Blade- oder Port-Info)

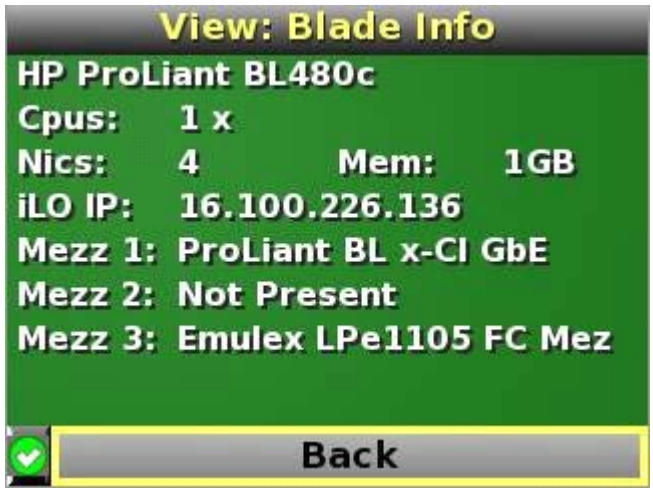
Der Bildschirm „Blade or Port Info“ (Blade- oder Port-Info) zeigt Informationen für einen bestimmten Server Blade an. Wählen Sie im ersten Bildschirm die Nummer des Server Blade, und drücken Sie

anschließend die Taste „OK“. Wählen Sie **Blade Info** (Blade-Info) oder **Port Info** (Port-Info), und drücken Sie „OK“.


View: Blade and Port Info
Use Up/Down to change value.
Then Right or OK to Nav Bar,
then OK for Blade or Port Info
Blade range: 1 to 16
Side: None, A or B
Blade # = 02
Side = A
Blade Info
Port Info
Back

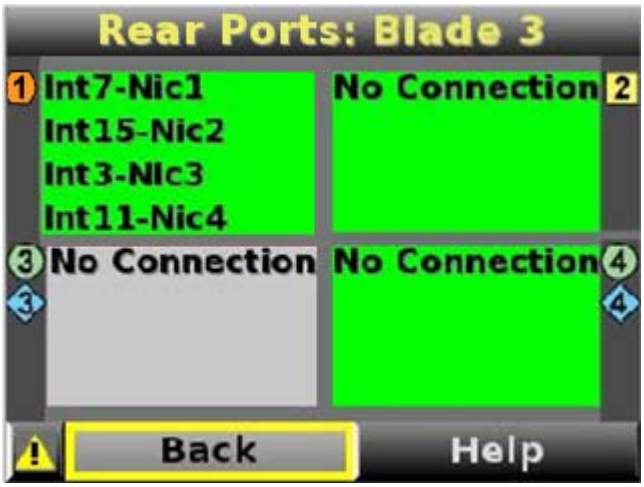
Wenn Sie einen BL2x220c-Server anzeigen, navigieren Sie rechts neben das zweite Auswahlfeld, und wählen Sie mit der Nach-oben- oder Nach-unten-Funktion Server A oder B aus. Die richtige Auswahl muss „N/A“ lauten, um alle anderen Server Blade-Infobildschirme auszuwählen.

Zur Anzeige von Informationen zum Server Blade wählen Sie **Blade Info** (Blade-Info), und drücken Sie die Taste „OK“.



Zur Anzeige der Ports, die von einem bestimmten Server Blade verwendet werden, wählen Sie **Port Info** (Port-Info), und drücken Sie die Taste „OK“.

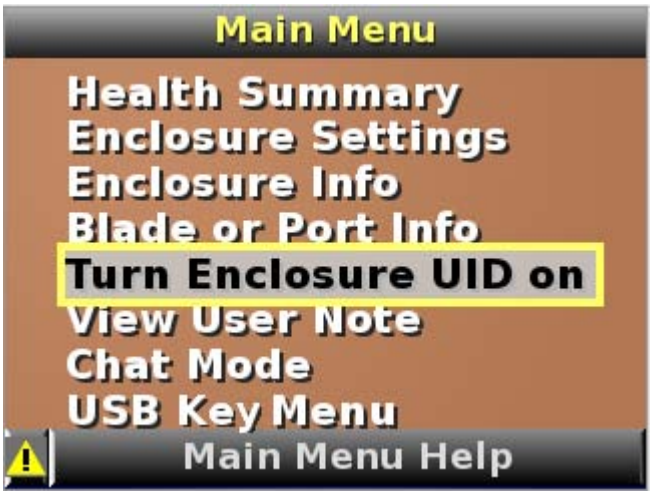
In dem unten dargestellten Server Blade mit voller Bauhöhe befinden sich vier integrierte NICs. Die anderen Verbindungsmoduleinschübe sind leer. Die vier integrierten NICs sind an bestimmte Port-Nummern an den Verbindungsmodulen angeschlossen.



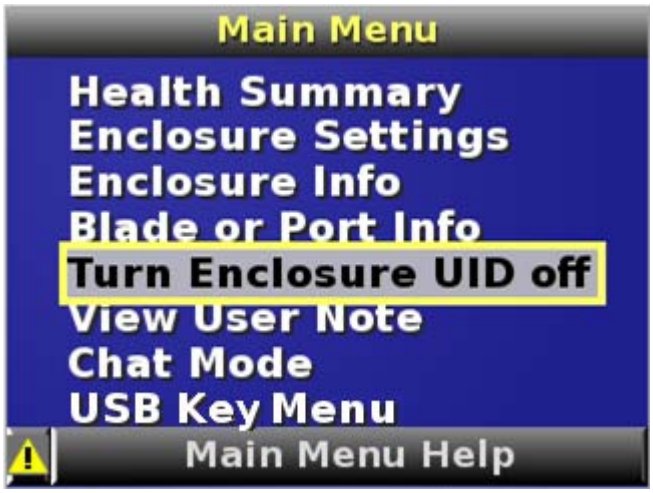
Bildschirm „Turn Enclosure UID On/Off“ (Gehäuse-UID aktivieren/deaktivieren)

Die Hauptmenüoption „Turn Enclosure UID Off“ (Gehäuse-UID deaktivieren) wird angezeigt, wenn die Gehäuse-UID aktiv ist, und „Turn Enclosure UID on“ (Gehäuse-UID aktivieren), wenn die Gehäuse-UID deaktiviert ist.

Die Auswahl der Option **Turn Enclosure UID On** (Gehäuse-UID aktivieren) im Hauptmenü schaltet die Gehäuse-UID-LED auf der Rückseite ein, und das Insight Display-Bildschirms wird blau.

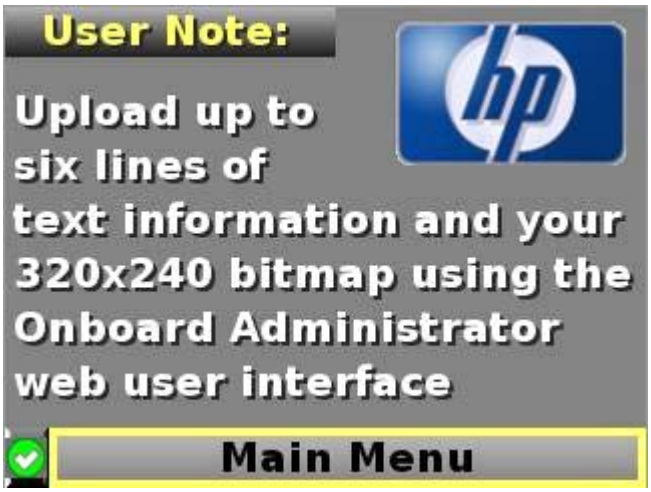


Die Auswahl der Option **Turn Enclosure UID Off** (Gehäuse-UID deaktivieren) im Hauptmenü schaltet die Gehäuse-UID-LED auf der Rückseite aus, und ändert die Farbe des Insight Display-Bildschirms, so dass sie den aktuellen Zustand reflektiert.



Bildschirm „View User Note“ (Benutzernotiz anzeigen)

Der Bildschirm „View User Note“ (Benutzernotiz anzeigen) zeigt sechs Textzeilen mit je maximal 25 Zeichen. Zeigen Sie mithilfe dieses Bildschirms nützliche Informationen wie die Telefonnummer des Ansprechpartners oder andere Daten an. Sie können diesen Bildschirm unter Verwendung der Remote-Onboard-Administrator-Web-Benutzerschnittstelle ändern. Sowohl Hintergrund als auch Text können geändert werden.


User Note:
Upload up to six lines of text information and your 320x240 bitmap using the Onboard Administrator web user interface
Main Menu

Bildschirm „Chat Mode“ (Chat-Modus)

Der Bildschirm „Chat Mode“ (Chat-Modus) wird vom Remote-Administrator verwendet, der über die Webschnittstelle eine Mitteilung an ein Gehäuse-Insight Display schickt. Der Techniker wählt über die Insight Display-Tasten einige vorbereitete Antworten aus oder wählt sich in eine benutzerdefinierte Antwortmitteilung auf der ?- Leitung ein. Um eine Antwort an den Administrator zurückzuschicken, platzieren Sie den Cursor auf der Schaltfläche **Send** (Senden) und drücken Sie anschließend die Taste **OK**.

Der Bildschirm „Chat Mode“ (Chat-Modus) besitzt oberste Priorität im Insight Display und wird so lange auf dem Bildschirm angezeigt, bis die Option **Send** (Senden) ausgewählt wird. Der Techniker kann diesen Chat-Bildschirm vorübergehend verlassen, um mit den anderen Insight Display-Bildschirmen zu arbeiten. Er kann dann vom Hauptmenü zum Bildschirm „Chat Mode“ zurückkehren, um eine Antwort zu verschicken. Nach erfolgter Antwort wird der Bildschirm „Chat Mode“ (Chat-

Modus) gelöscht. Sowohl Antwort A als auch Antwort ? werden anschließend dem Remote-Administrator in der Webschnittstelle für LCD-Chat angezeigt.

Bildschirm „USB Menu“ (USB-Menü)

Die Onboard Administrator-Firmware, Version 2.30 und höher, bietet zusätzliche Unterstützung für die folgenden USB-Schlüssel-Optionen:

- Aktualisieren der OA-Firmware
- Wiederherstellen der OA-Konfiguration
- Speichern der OA-Konfiguration

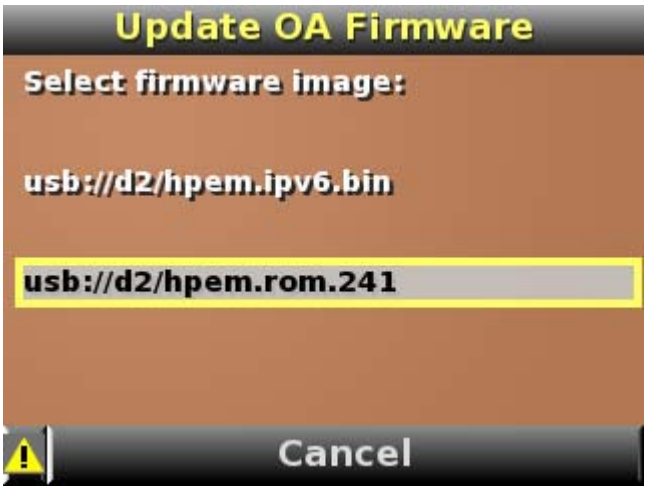
Onboard Administrator unterstützt USB-Schlüssel, die für die FAT32- oder EXT2-Dateisysteme formatiert sind. Die maximale unterstützte USB-Schlüsselgröße ist 4 GB. Sie können entweder den Anschluss am aktiven Onboard Administrator Modul auf der Vorderseite des Gehäuses oder einen USB-Anschluss am optionalen KVM-Modul verwenden.

So öffnen Sie das „USB Key Menu“ (USB-Schlüssel-Menü):

1. Stecken Sie einen USB-Schlüssel in das Onboard Administrator-Modul.
2. Wählen Sie im Hauptmenü die Option **USB Key Menu** (USB-Schlüssel-Menü).

Unter „USB Key Menu“ (USB-Schlüssel-Menü) sind die folgenden Optionen verfügbar:

- **Update OA Firmware** (OA-Firmware aktualisieren): Wählen Sie diese Option zum Aktualisieren der Firmware. Auf dem USB-Schlüssel muss sich ein Onboard Administrator-Firmware-Image mit einer BIN-Dateierweiterung befinden.



- **Restore Configuration** (Konfiguration wiederherstellen): Wählen Sie diese Option zum Hochladen einer Gehäuse-Konfigurationsdatei mit der Erweiterung „.CFG“.

  Das Menü „Restore OA Configuration“ (OA-Konfiguration wiederherstellen) führt alle Dateien auf dem angeschlossenen USB-Schlüssel mit der Dateierweiterung „.CFG“ auf. Wählen Sie die gewünschte Konfigurationsdatei aus, und drücken Sie **OK**.

  Da die Konfigurationsdatei Einstellungen wie z. B. die IP-Adresse von Onboard Administrator ändern kann, wenden Sie die gleiche Datei nur dann auf mehrere Gehäuse an, wenn die Einstellungen generisch sind, wie SNMP- oder LDAP-Serveradressen. Wenden Sie die gleiche Datei nicht auf mehrere Gehäuse an, wenn sie Befehle zur Konfiguration der Onboard Administrator-IP-Adresse oder EBIPA-IP-Adressbefehle enthält.

- **Save Configuration** (Konfiguration speichern): Wählen Sie diese Option aus, um die Gehäusekonfiguration in einer Datei auf dem USB-Schlüssel zu speichern.

Bildschirm „KVM Menu“ (KVM-Menü)

Wenn die Gehäuse-KVM-Funktion unterstützt wird, zeigt das Insight Display-Hauptmenü die Taste **KVM Menu** (KVM-Menü) an. Wählen Sie diese Schaltfläche, um das Insight Display zu deaktivieren

und den VGA-Anschluss am KVM-Modul zu aktivieren. Es kann nur jeweils eine der beiden Schnittstellen aktiv sein. Weitere Informationen finden Sie unter „Gehäuse-KVM“ („Gehäuse-KVM“ auf Seite 50).

Insight Display-Fehlermeldungen

Die Gehäuseinstallation ist erfolgreich, wenn alle Fehler korrigiert wurden. Die Fehler in den folgenden Abschnitten sind typisch für die Installation und die Erstkonfiguration des Gehäuses. Informationen zum Beseitigen der Fehler, die nach dem ersten Einschalten und Konfigurieren auftreten, finden Sie im *HP BladeSystem Onboard Administrator User Guide* (HP BladeSystem Onboard-Administrator Benutzerhandbuch).

Die folgenden Fehlerarten können bei der Installation und Konfiguration des Gehäuses auftreten:

- Stromversorgungsfehler
- Kühlungsfehler
- Positionsfehler
- Konfigurationsfehler
- Komponentenausfallfehler

Wenn die Gehäuse-UID-LED ausgeschaltet ist, leuchtet das Insight Display im Falle eines Fehlers gelb. Die Navigationsleiste zeigt die folgenden Auswahlmöglichkeiten bei einem Fehlerzustand an:

- Das Symbol „Health Summary“ (Zustand – Zusammenfassung) – Zeigt den Bildschirm „Health Summary“ (Zustand – Zusammenfassung) an.
- Fix THIS (DIESES Problem beheben) – Schlägt korrigierende Maßnahmen vor, um den aktuellen Fehler zu beseitigen.
- Next Alert (Nächste Alarmmeldung) – Zeigt die nächste Alarmmeldung oder, wenn keine vorhanden ist, den Bildschirm „Health Summary“ (Zustand – Zusammenfassung) an.
- Previous Alert (Vorherige Alarmmeldung) – Zeigt die vorherige Alarmmeldung an.

Stromversorgungsfehler

Stromversorgungsfehler können durch eine unzureichende Versorgungskapazität für ein Gehäuse verursacht werden und für Server Blades, Speicher-Blades oder Verbindungsmodule auftreten.

So korrigieren Sie einen Stromversorgungsfehler:

1. Wechseln Sie mit den Pfeiltasten zur Option **Fix This** (Dieses Problem beheben), und drücken Sie die Taste **OK**.
2. Lesen Sie die vom Insight Display vorgeschlagene korrigierende Maßnahme, und führen Sie sie durch. In den meisten Fällen müssen Sie entweder weitere Netzteile zum Gehäuse hinzufügen oder die angegebenen Komponenten entfernen.

Kühlungsfehler

Es kommt zu Kühlungsfehlern, wenn zu wenig Lüfter im Gehäuse installiert sind oder wenn die vorhandenen Lüfter nicht effektiv arbeiten. Kühlungsfehler können für Server Blades, Speicher-Blades oder Verbindungsmodule auftreten.

So korrigieren Sie einen Kühlungsfehler:

1. Wechseln Sie mit den Pfeiltasten zur Option **Fix This** (Dieses Problem beheben), und drücken Sie die Taste **OK**.
2. Lesen Sie die vom Insight Display vorgeschlagene korrigierende Maßnahme, und führen Sie sie durch. In den meisten Fällen müssen Sie entweder weitere Lüfter zum Gehäuse hinzufügen, die Lüfterkonfiguration korrigieren oder die angegebenen Komponenten entfernen.

Positionsfehler

Zu Positions-(Installations-)fehlern kommt es, wenn eine Komponente nicht im richtigen Einschub installiert wurde. Positionsfehler können für Server Blades, Speicher-Blades, Netzteile und Lüfter auftreten.

So korrigieren Sie einen Positionsfehler:

1. Wechseln Sie mit den Pfeiltasten zur Option **Fix This** (Dieses Problem beheben), und drücken Sie die Taste **OK**.
2. Lesen Sie die vom Insight Display vorgeschlagene korrigierende Maßnahme, und führen Sie sie durch. Entfernen Sie die angegebene Komponente, und installieren Sie sie im richtigen Einschub. Das Insight Display zeigt die richtige Einschubnummer an.

Konfigurationsfehler

Konfigurationsfehler werden dadurch verursacht, dass die Verbindungsmodule in den falschen Einschüben oder Mezzanine Cards in den falschen Steckplätzen im Server Blade installiert sind. Konfigurationsfehler können für Server Blades und Verbindungsmodule auftreten.

So korrigieren Sie einen Konfigurationsfehler:

1. Wechseln Sie mit den Pfeiltasten zur Option **Fix This** (Dieses Problem beheben), und drücken Sie die Taste **OK**.
2. Lesen Sie die vom Insight Display vorgeschlagene korrigierende Maßnahme, und führen Sie sie durch. Wählen Sie je nach Fehler eine der folgenden Vorgehensweisen:
   - Entfernen Sie das angegebene Verbindungsmodul, und installieren Sie es im richtigen Einschub (das Insight Display zeigt den richtigen Einschub an).
   - Entfernen Sie den Server Blade, um die Installation der Mezzanine Card zu korrigieren (das Insight Display zeigt den richtigen Steckplatz an). Informationen zur Installation der Mezzanine Card finden Sie im Benutzerhandbuch für den jeweiligen Server auf der Documentation CD.

Komponentenausfallfehler

Komponentenausfallfehler können auftreten, wenn eine Komponente ausgefallen ist.
Von Komponentenausfallfehlern können alle Komponenten betroffen sein, einschließlich:

- Server Blades
- Speicher-Blades
- Netzteile
- Verbindungsmodule
- Onboard Administrator-Module

- Lüfter
- Netzversorgungskomponenten

So korrigieren Sie einen Komponentenausfallfehler:

1. Wechseln Sie mit den Pfeiltasten zur Option **Fix This** (Dieses Problem beheben), und drücken Sie die Taste **OK**.
2. Lesen Sie die vom Insight Display vorgeschlagene korrigierende Maßnahme, und führen Sie sie durch. In den meisten Fällen müssen Sie die ausgefallene Komponente entfernen, um den Fehler zu beseitigen.
3. Ersetzen Sie die ausgefallene Komponente gegebenenfalls durch eine Ersatzkomponente.

HINWEIS: Wenn der Komponentenausfallfehler eine Netzversorgungskomponente betrifft, müssen Sie die ausgefallene Netzversorgungskomponente reparieren lassen, um den Fehler zu beseitigen.

4 Gehäuse-KVM

Funktionen

Die Gehäuse-KVM-Funktion ermöglicht es dem Onboard Administrator, zwischen Server-Videokonsolen umzuschalten, an die nur ein VGA-Monitor, eine USB-Tastatur und eine USB-Maus angeschlossen sind, ohne dass dazu ein PC erforderlich ist. Zusätzlich zum Starten und Ausführen von Servervideokonsolen bietet das Gehäuse-KVM-Menü Informationen zum Zustand jedes einzelnen Servers und ermöglicht es Ihnen, Server ein- und auszuschalten und Gehäuse-DVD an diese Server anzuschließen.

Das Insight Display ist deaktiviert (erscheint leer), solange die Gehäuse-KVM-Funktion aktiv ist. Im Gehäuse-KVM-Menü befindet sich eine Schaltfläche zum Aufruf der Insight Display-Bildschirme auf dem VGA-Monitor über die Cursortasten der Tastatur.

Das Gehäuse-KVM-Menü enthält auch eine Schaltfläche für die Auswahl der Onboard Administrator-Befehlszeilenschnittstellen-Konsole. Nachdem Sie sich über die Gehäuse-KVM-Funktion bei der Onboard Administrator-Befehlszeilenschnittstellen-Konsole angemeldet haben, können Sie auf alle Funktionen der Befehlszeilenschnittstelle zugreifen.

Für die KVM-Funktion muss beim c3000-Gehäuse das optionale KVM-Modul auf der Gehäuserückseite installiert sein. Dieses KVM-Modul stellt einen VGAAnschluss und zwei zusätzliche USB 2.0-Anschlüsse bereit. Für das c7000-Gehäuse erfordert diese Funktion das Onboard Administrator-Modul mit VGA-Anschluss.

Methoden zum Verwenden der Gehäuse-KVM-Funktion

Für die Verwendung der Gehäuse-KVM-Funktion wählen Sie eine der folgenden Methoden:

- Verbinden Sie den VGA-Anschluss direkt mit einem VGA-Monitor, und schließen Sie dann eine Tastatur und eine Maus an die USB-Anschlüsse an.
- Verbinden Sie den VGA-Anschluss über einen CAT5-KVM-USB-Adapter mit einem HP KVM-Switch und anschließend das USB-Kabel vom Adapter mit dem Onboard Administrator-USB-Anschluss.

HINWEIS: Sollten bei der Eingabe auf einer GUI-Textkonsole eines Linux-Systems Zeichenwiederholungsprobleme, dann müssen möglicherweise die folgenden Konfigurationseinstellungen geändert werden:

Stellen Sie für die Tastatur-Wiederholung/-Verzögerung 1000 ms (kbdrate –d 1000 im Server-Skript init) ein.

Konfigurieren Sie als automatische Wiederholungsrate der GUI 1 Sekunde.

Zugreifen auf das KVM-Menü

Rufen Sie das KVM-Menü durch Auswahl einer der folgenden Optionen auf:

- Drücken Sie auf einer am KVM-Modul angeschlossenen USB-Tastatur **Drucken** oder **S-Abf**.
- Drücken Sie auf einem VGA-Monitor mit einer Tastatur und Maus **Drucken**.
- Wenn das KVM-Modul über einen VGA- oder USB-Adapter an den KVM-Switch eines HP Racks angeschlossen ist, drücken Sie **Drucken**, um das KVM-Optionsmenü des HP Racks zu aktivieren. Drücken Sie erneut **Drucken**, um das KVM-Menü des Gehäuses anzuzeigen.

Wählen Sie den KVM-Anschluss des HP Racks, an den das Gehäuse angeschlossen ist, und drücken Sie die **Eingabetaste**, um das KVM-Menü des betreffenden Gehäuses auszuwählen. Sollte der Bildschirm leer sein, berühren Sie eine beliebige Taste auf der Tastatur, um das KVM-Menü zu aktivieren und das Insight Display des Gehäuses zu deaktivieren.

Das Insight Display wird leer angezeigt, wenn das Gehäuse-KVM-Menü aktiv ist.

Zurückkehren zum KVM-Menü von einer anderen Schnittstelle

Um von einer Server-Konsolen-, Insight Display- oder OA CLI-Anzeige zum KVM-Menü zurückzukehren, drücken Sie die Taste **Drucken** auf der USB-Tastatur.

Zurückkehren zum Insight Display über das KVM-Menü

Um das Insight Display wiederherzustellen und ein leeres KVM-Menü anzuzeigen (eine kurze Verzögerung ist möglich), drücken Sie eine beliebige Insight Display-Taste oder wählen Sie im KVM-Menü **Exit KVM** (KVM beenden) aus.

Navigieren zum KVM-Menü

Die folgende Abbildung zeigt das KVM-Menü:

HP KVM Menu Enclosure: c3000-E05 Rack: CT001
Press Sys Rq or Prt Sc key to return to this KVM Menu from other screens.
If you are also using an HP KVM switch, you have to press Prt Sc twice.
Status Bay# - Server Name
1 - YOUR-ESFCNZWOXG
2 - ORACLE-006
3 - ORACLE-007
4 - EXCHANGE-2
5 - ORACLE-009
6 - DHCP2
7 - LICENSE-SRV1
8 - CITRIX-1-24
Insight Display
OA CLI Console
Exit KVM
HELP

Zum Navigieren im HP KVM-Menü verwenden Sie die Pfeiltasten auf der Tastatur. Drücken Sie die **Eingabetaste** auf der Tastatur, um eine Menüaktion auszuwählen.

Zu den verfügbaren Aktionen gehören:

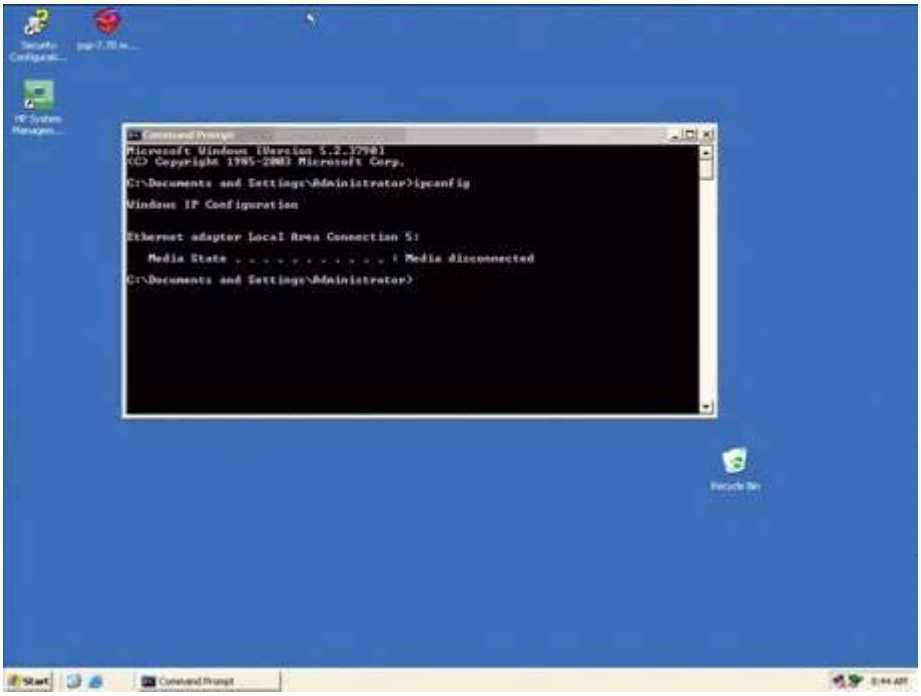
- Netzsymbol: Ändert den Stromversorgungszustand des Servers.
- DVD-Symbol: Ändert den Gehäuse-DVD-Status für den Server.
- Server Name (Servername): Stellt eine Verbindung zur Vollbildanzeige der Server-KVM-Konsole mit Tastatur- und Mausunterstützung her. Drücken Sie zur Rückkehr zum KVM-Menü die Taste **Drucken** oder **S-Abf**.
- Insight Display: Über den KVM-Monitor und die Pfeiltasten und die **Eingabetaste** auf der Tastatur kann das Insight Display bedient werden.
- OA CLI-Konsole: Über den KVM-Monitor und die Tastatur kann auf OA CLI-Befehle zugegriffen werden.

- Exit KVM (KVM beenden): Deaktiviert den KVM-Monitor und aktiviert das Insight Display des Gehäuses.
- Help (Hilfe): Zeigt einen HP KVM-Hilfebildschirm mit Informationen zu den Statussymbolen und zu dem KVM-Betrieb an.

Ist die LCD-PIN festgelegt, sind die gesamte Stromversorgung des Servers und alle DVD-Steuerelemente des Servers durch die LCD-PIN geschützt. Die Server-Konsole und die Onboard Administrator-CLI sind durch Benutzeranmeldungen geschützt.

Das KVM-Menü enthält die folgenden Optionen:

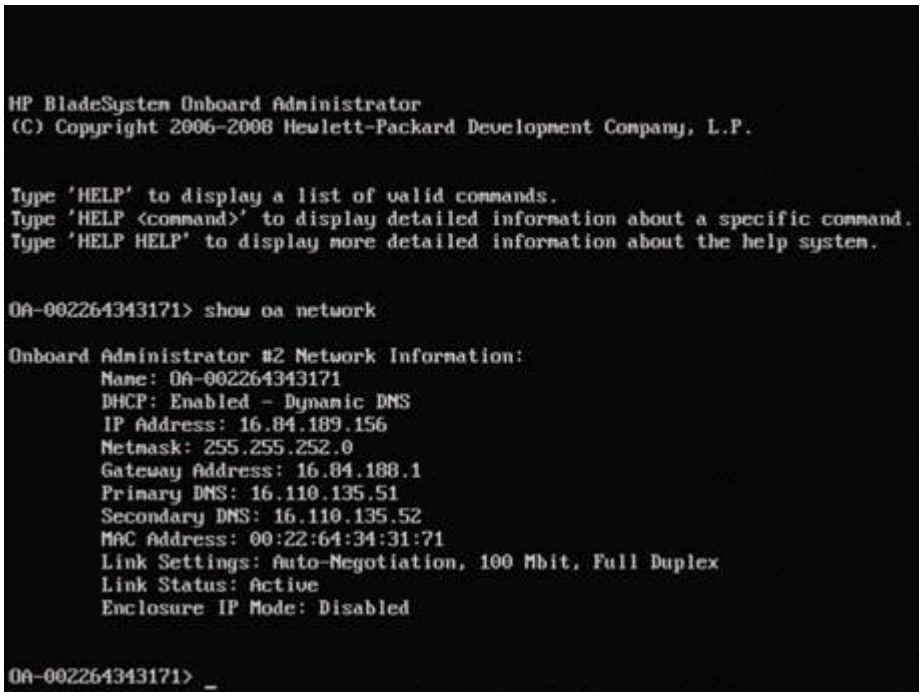
- Server Console (Server-Konsole): Wählen Sie eine Serverkonsole durch Auswahl des Servernamens aus. Die ausgewählte Serverkonsole ist eine Vollbildgrafik oder Text, je nach der aktuellen Umgebung auf dem betreffenden Server. Bis auf „Drucken“ werden alle Tastenanschläge der KVM-Tastatur zusammen mit Tastenklicks der KVM-Maus zum Server gesendet. Drücken Sie **Drucken**, um die Serverkonsole zu beenden und zum KVM-Menü zurückzukehren.


Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 5:
Media State . . . . . : Media disconnected
C:\Documents and Settings\Administrator>

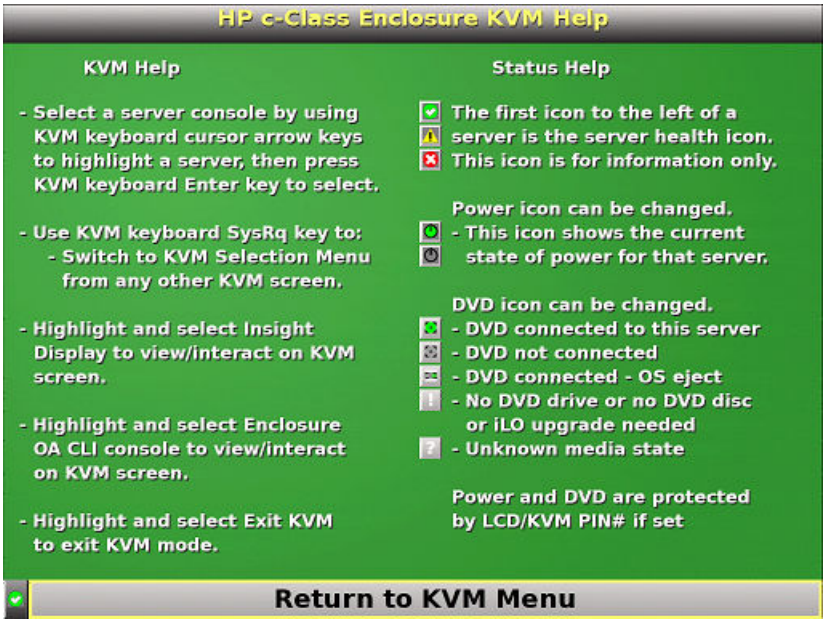
HINWEIS: Bei den Auflösungen 1024x768 bis 1600x1200 entspricht die Bildschirmauflösung der Auflösung des Serverkonsolen-Bildschirms. Serverkonsolen-Auflösungen unterhalb 1024x768 führen zur Anzeige auf einem Teil des Onboard Administrator-KVM-Bildschirms im Modus 1024x768. Bei Serverkonsolen-Auflösungen oberhalb von 1600x1200 wird eine Warnmeldung angezeigt, und Sie gelangen wieder zum Bildschirm des Gehäuse-KVM-Menüs.

- Server Power (Server-Stromversorgung): Wählen Sie dieses Stromversorgungssymbol für einen Server aus, um den Stromversorgungszustand des Servers zu ändern.
- Server DVD (Server-DVD): Wählen Sie dieses DVD-Symbol für einen Server, um die Gehäuse-DVD-Verbindung für den betreffenden Server zu ändern.
- Server Health (Server-Zustand): Wählen Sie dieses Zustandssymbol aus, um den aktuellen Zustand des betreffenden Servers anzuzeigen.
- Insight Display: Wählen Sie die Schaltfläche „Insight Display“, um vom KVM-Menü aus auf Insight Display-Bildschirme zuzugreifen.

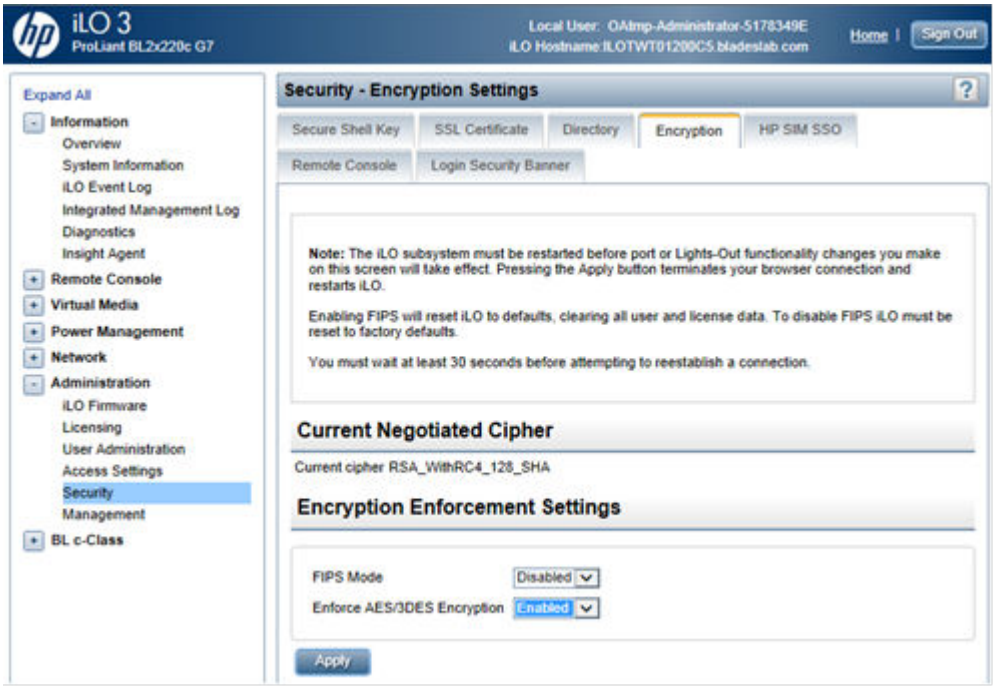
- OA CLI: Wählen Sie **OA CLI**, um die Onboard Administrator-CLI aufzurufen. Melden Sie sich mit der KVM-Tastatur bei dem Onboard Administrator an. Damit wird eine Textkonsole im Vollbildformat für die aktive Onboard Administrator-CLI aufgerufen. Drücken Sie **Drucken**, um die Onboard Administrator-CLI-Konsole zu beenden und zum KVM-Menü zurückzukehren.


HP BladeSystem Onboard Administrator
(C) Copyright 2006-2008 Hewlett-Packard Development Company, L.P.
Type 'HELP' to display a list of valid commands.
Type 'HELP <command>' to display detailed information about a specific command.
Type 'HELP HELP' to display more detailed information about the help system.
OA-002264343171> show oa network
Onboard Administrator #2 Network Information:
Name: OA-002264343171
DHCP: Enabled - Dynamic DNS
IP Address: 16.84.189.156
Netmask: 255.255.252.0
Gateway Address: 16.84.188.1
Primary DNS: 16.110.135.51
Secondary DNS: 16.110.135.52
MAC Address: 00:22:64:34:31:71
Link Settings: Auto-Negotiation, 100 Mbit, Full Duplex
Link Status: Active
Enclosure IP Mode: Disabled
OA-002264343171> _

- Help (Hilfe): Wählen Sie **Help** (Hilfe) um die KVM-Hilfeinformationen anzuzeigen.


HP c-Class Enclosure KVM Help
KVM Help
- Select a server console by using KVM keyboard cursor arrow keys to highlight a server, then press KVM keyboard Enter key to select.
- Use KVM keyboard SysRq key to:
- Switch to KVM Selection Menu from any other KVM screen.
- Highlight and select Insight Display to view/interact on KVM screen.
- Highlight and select Enclosure OA CLI console to view/interact on KVM screen.
- Highlight and select Exit KVM to exit KVM mode.
Status Help
The first icon to the left of a server is the server health icon.
This icon is for information only.
Power icon can be changed.
- This icon shows the current state of power for that server.
DVD icon can be changed.
- DVD connected to this server
- DVD not connected
- DVD connected - OS eject
- No DVD drive or no DVD disc or iLO upgrade needed
- Unknown media state
Power and DVD are protected by LCD/KVM PIN# if set
Return to KVM Menu

HINWEIS: Wenn sich Onboard Administrator im FIPS-Modus befindet, muss die iLO-Einstellung für den Sicherheitszugriff, „Enforce AES/3DES Encryption“ (AES/3DES-Verschlüsselung erzwingen), aktiviert sein. Um die iLO-Einstellung zu ändern, navigieren Sie zu **Administration>Security>Encryption** (Administration>Sicherheit>Verschlüsselung). Die KVM-Verbindung mit iLO2 wird im FIPS-Modus ON/DEBUG nicht unterstützt.



5 Assistent für die Erstkonfiguration (First Time Setup Wizard)

Bevor Sie beginnen

Bevor Sie den Assistenten für die Erstkonfiguration ausführen, müssen Sie:

1. Die Onboard Administrator-Module installieren.
2. Die Onboard Administrator-Module an das Netzwerk anschließen.
3. Den Insight Display-Installationsassistenten abschließen. Konfigurieren Sie mindestens die IP-Adresse des aktiven Onboard Administrator-Moduls.
4. Die Insight Display-Installation durchführen.

Anmelden bei Onboard Administrator

1. Öffnen Sie einen Browser, und stellen Sie über die IP-Adresse, die im Insight Display-Installationsassistenten konfiguriert wurde, eine Verbindung zum aktiven HP BladeSystem Onboard Administrator-Modul her.
2. Geben Sie den Benutzernamen und das anfängliche Administratorkennwort für Ihr HP BladeSystem Onboard Administrator-Konto ein, das auf dem am Onboard Administrator-Modul angebrachten Aufkleber zu finden ist.

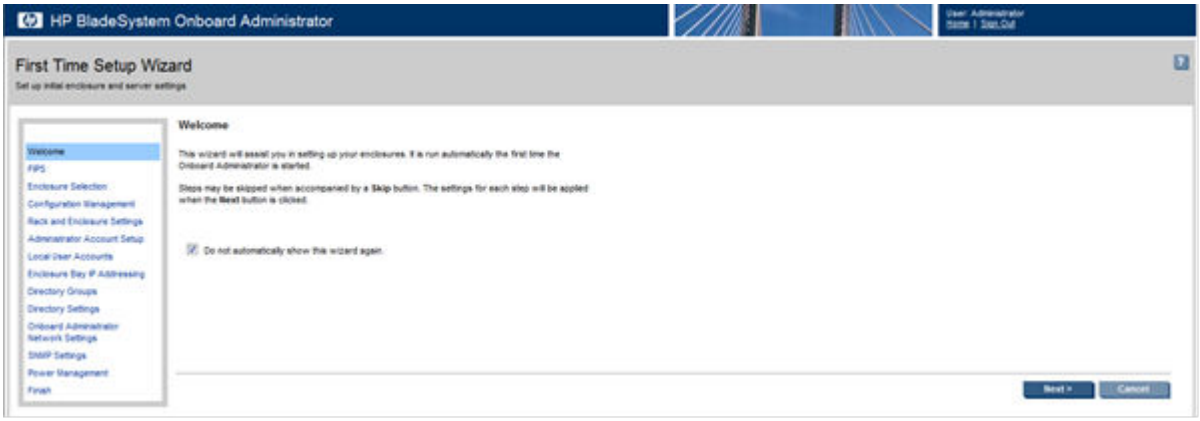
Probleme, die beim Anmelden auftreten können:

- Sie haben die Informationen nicht richtig eingegeben. Die Groß-/Kleinschreibung des Kennworts wird berücksichtigt.
- Die eingegebenen Kontoinformationen wurden nicht für HP BladeSystem Onboard Administrator konfiguriert.
- Der angegebene Benutzername wurde gelöscht, deaktiviert oder gesperrt.
- Das Kennwort für das Konto muss geändert werden.
- Sie versuchen, sich über eine IP-Adresse anzumelden, die für das betreffende Konto nicht gültig ist.
- Wenn die Probleme weiterhin bestehen, wenden Sie sich an Ihren Administrator.

Bei der erstmaligen Anmeldung führt der Onboard Administrator automatisch den Assistenten für die Erstkonfiguration „First Time Setup Wizard“ aus.

Klicken Sie im Konfigurationsassistenten auf **Next** (Weiter), um Ihre Änderungen zu speichern und zum nächsten Schritt zu wechseln. Klicken Sie auf **Skip** (Überspringen), um einen Schritt zu überspringen, ohne irgendwelche Änderungen zu speichern.

Sie können zu vorhergehenden Schritten im Assistenten zurückkehren, indem Sie sie in der linken Strukturansicht auswählen. Sie können den Assistenten jederzeit erneut ausführen, indem Sie ihn im Menü „Wizards“ (Assistenten) auswählen.



Benutzereinstellungen

Um die Anzeigesprache zu ändern, wählen Sie eine Anzeigesprache aus der Dropdownliste aus, und klicken Sie dann auf **Apply** (Übernehmen). Die ausgewählte Sprache übersteuert die aktuelle Spracheinstellung des Browsers und wird bei nachfolgenden GUI-Sitzungen mit dem gleichen Onboard Administrator beibehalten. Die Einstellung gilt jedoch nicht für GUI-Sitzungen mit anderen Onboard Administrator-Modulen. (Die Einstellung beruht auf einem Cookie, das nur für die aktuelle Onboard Administrator-IP-Adresse gültig ist. Wenn sich die IP-Adresse ändert, muss die Einstellung erneut über die neue Adresse übernommen werden.)

Wenn die Sprache für Verbindungen zu anderen Onboard Administrator-GUIs, die von diesem Browser Gebrauch machen, angezeigt werden soll:

1. Fügen Sie die Sprache am Anfang der Liste der vom Browser bevorzugten Sprachen hinzu.
2. Wählen Sie auf dem Onboard Administrator-Bildschirm „User Preferences“ (Benutzereinstellungen) aus der Dropdownliste den Eintrag „Use browser settings“ (Browsereinstellungen verwenden) aus.
3. Aktualisieren Sie durch Klicken auf **Apply** (Übernehmen) die Anzeigesprache. Auf den anderen Onboard Administrator-Modulen muss das entsprechende Sprachpaket installiert sein. Weitere Informationen zum Installieren eines Sprachpakets finden Sie auf der Registerkarte „Language Pack“ (Sprachpaket) des aktiven Onboard Administrator-Moduls.

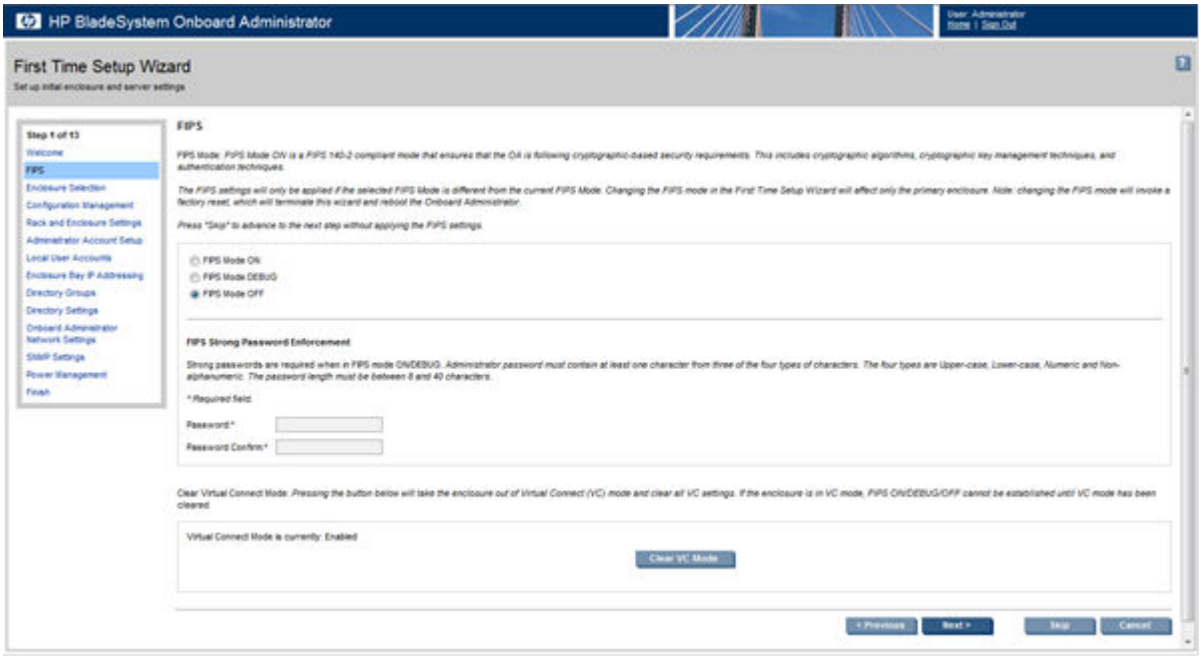
   Sollte bereits „Use browser settings“ (Browsereinstellungen verwenden) eingestellt sein, dann aktualisieren Sie die Anzeigesprache durch Klicken auf **Refresh** (Aktualisieren), ohne die Einstellung zu ändern.

Die Dropdownliste „User Preferences“ (Benutzereinstellungen) enthält nur die Sprachen, die auf dem Onboard Administrator installiert oder integriert sind. Wenn Sie als Browsersprache eine Sprache einstellen, die nicht aufgelistet wird, verwendet die Onboard Administrator-GUI nicht die Browser-Spracheinstellung, sondern stattdessen die GUI-Standardsprache (Englisch).

HINWEIS: Sollte die Anzeigesprache nicht korrekt geladen werden, dann löschen Sie das Browsercache und aktualisieren Sie die Anwendung durch Aktualisieren oder Neuladen des Browsers.

HINWEIS: Wenn ein installiertes Sprachpaket mit der Onboard Administrator-GUI verwendet wird und der Browser nicht alle Zeichen richtig anzeigt, stellen Sie sicher, dass im Betriebssystem die entsprechende Sprachunterstützung installiert ist.

FIPS



FIPS-Modus

HINWEIS: Änderungen des FIPS-Modus in ON/DEBUG oder OFF werden nur wirksam, wenn der VC-Modus deaktiviert ist.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

- **FIPS Mode OFF** (FIPS-Modus AUS): Ermöglicht die Verwendung von nicht FIPS-140-2-genehmigten Algorithmen.
- **FIPS Mode ON** (FIPS-Modus EIN): Erzwingt die Verwendung von Onboard Administrator in einem FIPS 140-2-genehmigten Modus. Diese Einstellung unterstützt die Verwendung von genehmigten kryptographischen Protokollen und Chiffren.
- **FIPS Mode DEBUG** (FIPS-Modus DEBUG): Stellt den Onboard Administrator auf eine Umgebung ähnlich dem FIPS-Modus ON ein, jedoch mit optionaler Debug-Unterstützung von HP. Der FIPS-Modus DEBUG besitzt die Funktionalität des FIPS-Modus ON, wird aufgrund der Debug-Option jedoch nicht als FIPS-konform angesehen.

Nach Vornahme aller Änderungen wird Onboard Administrator neu gestartet.

HINWEIS: Wenn dieser Vorgang ausgeführt wird, gehen alle bestehenden Einstellungen verloren. Bei einer Änderung der FIPS-Modus-Einstellung wird der Vorgang „Restore to Factory Default“ (Auf Werkseinstellungen zurücksetzen) durchgeführt.

HINWEIS: Sorgen Sie im FIPS-Modus ON/DEBUG dafür, dass ein starkes Kennwort festgelegt wurde.

Statussymbole des FIPS-Modus

Wenn der FIPS-Modus ON oder DEBUG aktiviert ist, wird der aktuelle Status des FIPS-Modus durch ein Symbol in der Onboard Administrator-Kopfleiste auf den GUI-Bildschirmen angezeigt. Er wird

auch auf der Onboard Administrator-Anmeldeseite in der Spalte „Connection“ (Verbindung) der Gehäusetabelle angezeigt. Die Statussymbole werden in der folgenden Tabelle beschrieben:

Symbol des FIPS-Modus	Beschreibung
	Der FIPS-Modus ist aktiviert (ON).
	Für den FIPS-Modus ON sind eine oder mehrere Warnungen vorhanden. Bewegen Sie den Mauszeiger über das Symbol, um zu bestimmen, um welche Art von Warnung es sich handelt.
	Der FIPS-Modus DEBUG ist aktiviert.
	Für den FIPS-Modus DEBUG sind eine oder mehrere Warnungen vorhanden. Bewegen Sie den Mauszeiger über das Symbol, um zu bestimmen, um welche Art von Warnung es sich handelt.

Erzwingung von starken FIPS-Kennwörtern

Wenn zwischen den verfügbaren FIPS-Modi gewechselt wird, werden starke Kennwörter aktiviert, werden als Mindestkennwortlänge acht Zeichen festgelegt und wird ein neues Kennwort für das Administratorkonto angefordert. Außerdem werden beim Wechsel zu FIPS-Modus ON oder FIPS-Modus DEBUG der Gehäuse-IP-Modus und Telnet sowie SNMPv1- und SNMPv2-Protokolle deaktiviert, und SNMPv3 ist verfügbar.

Um die Einstellungen zu speichern, klicken Sie auf **Next** (Weiter). Im Fall verbundener Gehäuse wirkt sich dies nur auf das primäre Gehäuse aus. Um mit dem nächsten Schritt fortzufahren, ohne die FIPS-Einstellungen zu übernehmen, klicken Sie auf **Skip** (Überspringen).

HINWEIS: Beim Aufrufen und Beenden des FIPS-Modus werden die Werkseinstellungen wiederhergestellt und wird das Insight Display (LCD) gesperrt. Wenn der Onboard Administrator zuvor mit einer statischen IP-Adresse konfiguriert war, wird standardmäßig eine DHCP-Adresse eingestellt, bis er mit einer statischen IP-Adresse neu konfiguriert wird. Für eine Wiederherstellung ist Zugriff auf die serielle Onboard Administrator-Konsole zum Ausführen des Befehls `SHOW OA NETWORK` erforderlich, mit dem die neue Onboard Administrator-IP-Adresse ermittelt wird.

Der Begriff „FIPS-Modus“ wird in diesem Dokument und im Produkt zur Beschreibung der Funktion und nicht ihres Validierungsstatus verwendet. Da der FIPS-Prüfvorgang aufwändig ist, werden nicht alle Versionen geprüft. Informationen zum aktuellen FIPS-Status dieser oder einer beliebigen anderen Firmwareversion finden Sie in den folgenden Dokumenten:

- Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Modules In Process List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf)
- FIPS 140-1 and FIPS 140-2 Vendor List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

Löschen des VC-Modus

Bei Löschen des VC-Modus werden alle VC-Einstellungen vom Gehäuse gelöscht. Schalten Sie vor Löschen des VC-Modus alle VC-konfigurierten Server aus. Server, die nicht ausgeschaltet werden, behalten möglicherweise ihre VC-Einstellungen bei, bis sie neu gestartet werden. Der VC-Modus muss gelöscht werden, bevor zum FIPS-Modus OFF/ON/DEBUG gewechselt wird.

So löschen Sie den VC-Modus:

1. Klicken Sie auf **Clear VC Mode** (VC-Modus löschen). Es wird ein Bestätigungsbildschirm mit folgender Meldung angezeigt: `All servers should be powered off and not`

```
configured by Virtual Connect prior to clearing VC mode. Are you sure
that you wish to clear VC mode? (Vor Löschen des VC-Modus sollten alle
Server ausgeschaltet und nicht durch Virtual Connect konfiguriert
sein. Soll der VC-Modus wirklich gelöscht werden?)
```

2. Klicken Sie auf **OK**.

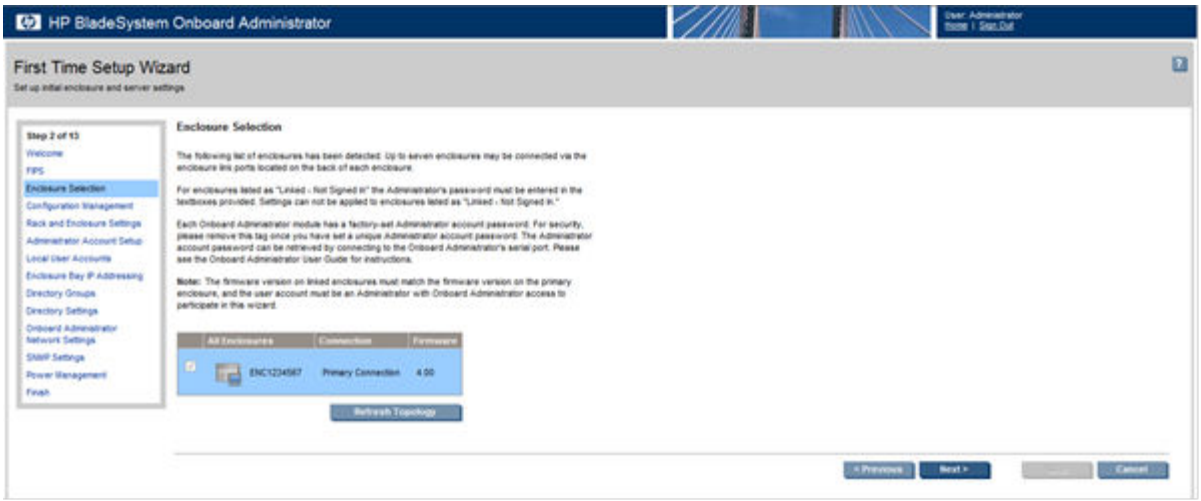
Erweiterte Sicherheitseinstellungen

Ausgewählte Sicherheitsprotokolle und Chiffren können über die Registerkarte **Enclosure Settings (Gehäuseeinstellungen)>Network Access (Netzwerkzugriff)>FIPS** aktiviert bzw. deaktiviert werden (Registerkarte „FIPS“ auf Seite 140).

Bildschirm „Enclosure Selection“ (Gehäuseauswahl)

Der Bildschirm „Enclosure Selection“ (Gehäuseauswahl) zeigt alle erkannten Gehäuse an und wählt standardmäßig das aktive Gehäuse aus, d. h. das Gehäuse, bei dem Sie angemeldet sind. Mit dem Kontrollkästchen neben jedem Gehäuse können Sie das betreffende Gehäuse auswählen oder dessen Auswahl aufheben. Um das Kontrollkästchen für alle Gehäuse auszuwählen oder dessen Auswahl aufzuheben, wählen Sie das Kontrollkästchen **All Enclosures** (Alle Gehäuse).

Um die Rack-Topologie zu aktualisieren, klicken Sie auf **Refresh Topology** (Topologie aktualisieren). Wenn **Refresh Topology** (Topologie aktualisieren) ausgewählt wird, wird anstelle des Bildschirms „Enclosure Selection“ (Gehäuseauswahl) der Modus „Linked“ („Verbunden“) angezeigt, und alle verbundenen Gehäuse werden angezeigt.



Verbundene Gehäuse haben einen der folgenden Zustände:

- Linked—Not Signed In (Verbunden – nicht angemeldet): Wählen Sie das Gehäuse aus, und geben Sie in das Kennwort-Textfeld das Administratorkennwort ein. Um das Gehäuse zu authentifizieren, klicken Sie auf **Next** (Weiter).
- „Linked—Not Signed In“ (Verbunden – Nicht angemeldet): Mit Kartenlesersymbol. Dieser Zustand gibt an, dass für das verbundene Gehäuse die 2-Faktor-Authentifizierung aktiviert ist, es aber nicht authentifiziert wurde. Dieser Zustand tritt unter zwei Bedingungen auf:
  - Wenn die Konfiguration nicht unterstützt wird. Für das primäre Gehäuse muss die 2-Faktor-Authentifizierung aktiviert sein und für das primäre und das verbundene Gehäuse müssen die gleichen Anmeldeinformationen gelten, damit das verbundene Gehäuse mit der 2-Faktor-Authentifizierung authentifiziert wird. Wenn die 2-Faktor-Authentifizierung für das

primäre Gehäuse nicht aktiviert ist, kann das verbundene Gehäuse nicht mit aktivierter 2-Faktor-Authentifizierung ausgewählt werden.

- Wenn Sie bei einem Gehäuse mit aktivierter 2-Faktor-Authentifizierung auf den Link „Sign Out“ (Abmelden) klicken, wird dieser Zustand angezeigt. Bei Auswahl dieses Gehäuses wird bei Anklicken der Schaltfläche **Next** (Weiter) ein Authentifizierungsversuch unternommen.

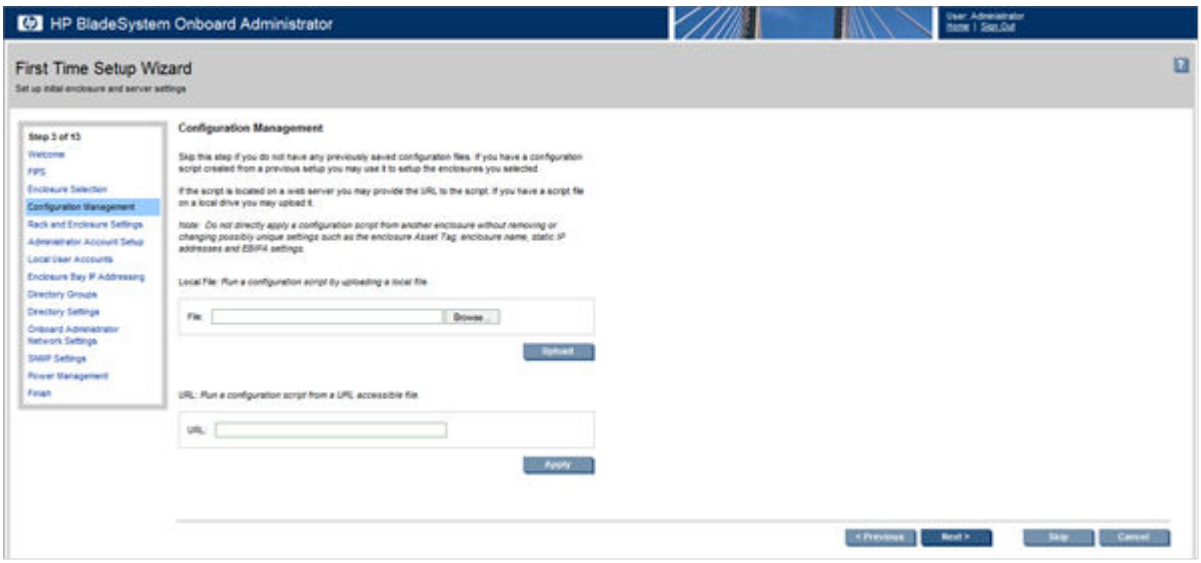
- „Linked—Signed In“ (Verbunden – Angemeldet): Mit oder ohne Kartenlesersymbol. Dieser Zustand besagt, dass das verbundene Gehäuse authentifiziert ist. Sofern die Gehäuseinformationen nicht bereits geladen wurden, werden sie beim Klicken auf **Next** (Weiter) geladen.

Werden auf dem Bildschirm „Enclosure Selection“ (Gehäuseauswahl) mehrere Gehäuse aufgelistet, wählen Sie das zu konfigurierende Gehäuse aus, und klicken Sie anschließend auf **Next** (Weiter).

Mögliche Werte sowie eine Beschreibung der einzelnen Felder finden Sie auf dem Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) (Bildschirm „Enclosure Information“ (Gehäuseinformationen) auf Seite 111).

Bildschirm „Configuration Management“ (Konfigurationsverwaltung)

Der Bildschirm „Configuration Management“ (Konfigurationsverwaltung) ermöglicht die Konfiguration der ausgewählten Gehäuse mithilfe einer Konfigurationsdatei, die von einer früheren Konfiguration gespeichert wurde. Sie können Skripte für mehrere Onboard Administrator-Module ausführen, bevor Sie den aktuellen Bildschirm verlassen.



So konfigurieren Sie ausgewählte Gehäuse mithilfe einer Konfigurationsdatei:

Wählen Sie das Gehäuse aus, auf das die Konfigurationsdatei hochgeladen werden soll. Die Konfigurationsdatei kann selbst dann nur auf ein Gehäuse hochgeladen werden, wenn auf dem Bildschirm **Enclosure Selection** (Gehäuseauswahl) die Option **All Enclosures** (Alle Gehäuse) ausgewählt wurde. Sie können eine lokale Datei, einen URL oder eine USB-Datei auswählen:

- **Local file** (Lokale Datei): Durchsuchen Sie die Verzeichnisstruktur nach der Konfigurationsdatei oder geben Sie den Pfad der Konfigurationsdatei in das Textfeld ein. Die maximale Anzahl von

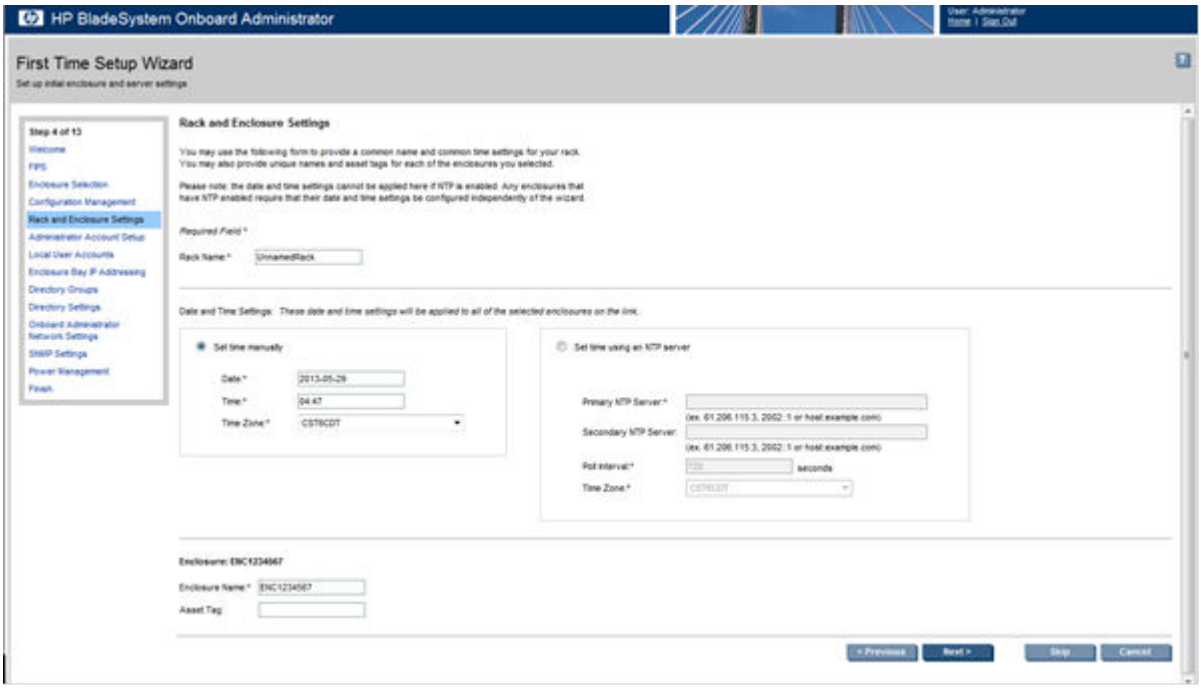
Zeichen im Dateipfad ist 256. Geben Sie den Pfad für die Konfigurationsdatei ein, und klicken Sie auf **Upload** (Hochladen).

- **URL**: Wenn sich die Konfigurationsdatei auf einem Webserver befindet, geben Sie einen HTTP-Pfad zur Datei ein. Die maximale Anzahl von Zeichen im Dateipfad ist 256. Klicken Sie nach der Eingabe der URL auf **Apply** (Übernehmen).
- **USB file** (USB-Datei): Sie können eine Konfigurationsdatei auf einem am Gehäuse angeschlossenen USB-Schlüssel auswählen. Wählen Sie die betreffende Konfigurationsdatei aus der Dropdown-Liste aus. Klicken Sie nach Auswahl der Konfigurationsdatei auf **Apply** (Übernehmen). Diese Option wird nur angezeigt, nachdem ein USB-Schlüssel an das Gehäuse angeschlossen wurde.

Nachdem ein Speicherort für die Datei ausgewählt wurde, werden die Ergebnisse in einem Dialogfeld angezeigt.

Bildschirm „Rack and Enclosure Settings“ (Rack- und Gehäuseeinstellungen)

In diesem Formular können Sie dem Rack Zeiteinstellungen und einen Eigennamen und den Gehäusen eindeutige Namen und Systemkennungen zuweisen.



Feld	Möglicher Wert	Beschreibung
Rack Name (Rack-Name)	1 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Der Name des Racks, in dem das Gehäuse installiert ist.
Date and Time Settings (Datum- und Uhrzeit-Einstellungen)	• Set time manually (Zeit manuell einstellen)	Die Methode, mit der Datum und Uhrzeit allen auf dem Link ausgewählten Gehäusen zugewiesen werden.

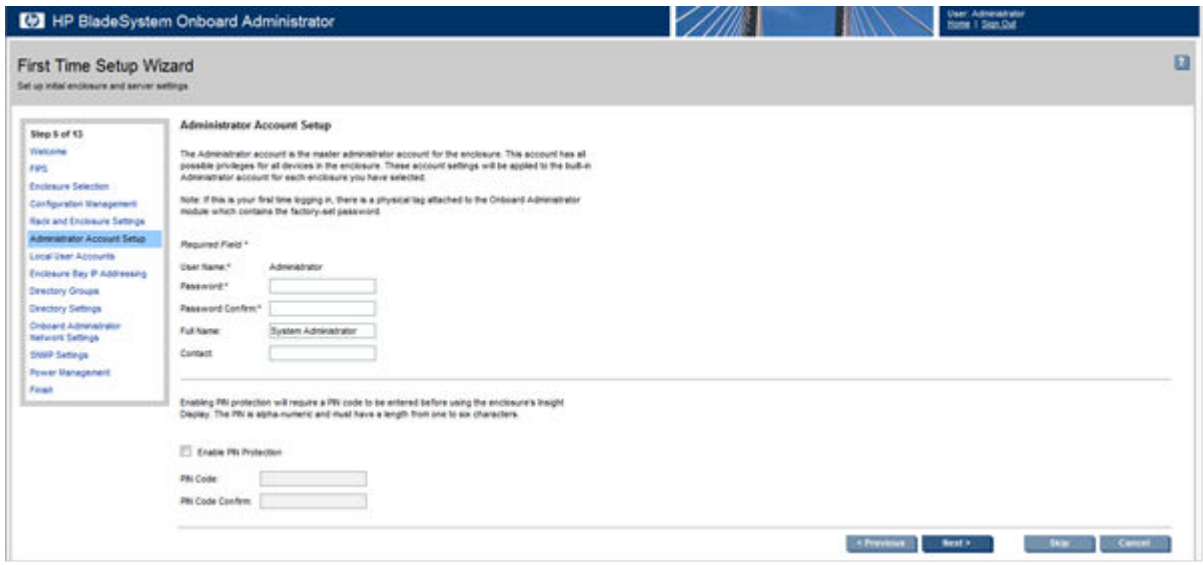
Feld	Möglicher Wert	Beschreibung
	• Set time using an NTP server (Zeit über einen NTP-Server einstellen)	
Date (Datum)	JJJJ-MM-TT, wobei: • MM ist eine ganze Zahl von 1 bis 12 • TT ist eine ganze Zahl von 1 bis 31	Das aktuelle Datum, das dem Gehäuse zugewiesen wurde.
Time (Uhrzeit)	HH:MM (24-Stunden-Format) • HH ist eine ganze Zahl von 0 bis 23 • MM ist eine ganze Zahl von 0 bis 59	Die aktuelle Uhrzeit, die dem Gehäuse zugewiesen wurde.
Time Zone (Zeitzone)	Zeitzoneneinstellungen • Zeitzoneneinstellungen für Afrika (Zeitzoneneinstellungen für Afrika auf Seite 428) • Zeitzoneneinstellungen für Amerika (Zeitzoneneinstellungen für Amerika auf Seite 429) • Zeitzoneneinstellungen für Asien (Zeitzoneneinstellungen für Asien auf Seite 431) • Zeitzoneneinstellungen für die Universalzeit (Zeitzoneneinstellungen für die Universalzeit auf Seite 428) • Zeitzoneneinstellungen für Ozeanien (Zeitzoneneinstellungen für Ozeanien auf Seite 432) • Zeitzoneneinstellungen für Europa (Zeitzoneneinstellungen für Europa auf Seite 433) • Zeitzoneneinstellungen für Polar-Zeit (Zeitzoneneinstellung	Die aktuelle Zeitzone, die dem Gehäuse zugeordnet wurde.

Feld	Möglicher Wert	Beschreibung
	en für Polar-Zeit auf Seite 433)	
Primary NTP Server (Primärer WINS-Server)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-).	IP-Adresse oder DNS-Name des primären NTP-Servers, der Datums- und Uhrzeitinformationen liefert.
Secondary NTP Server (Sekundärer WINS-Server)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-).	IP-Adresse oder DNS-Name des sekundären NTP-Servers, der Datums- und Uhrzeitinformationen liefert.
Poll Interval (Abfrageintervall)	Eine ganze Zahl von 60 bis 86400	Das Intervall, in dem der NTP-Server in Sekunden abgefragt wird.
Enclosure Name (Gehäusename)	1 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Der Name des ausgewählten Gehäuses.
Asset Tag (Systemkennung)	0 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Die Systemkennung wird zur Bestandskontrolle verwendet. Die Standardsystemkennung ist leer.

Informationen zum Anschließen von Gehäusen finden Sie im *HP BladeSystem c7000-Benutzerhandbuch*.

Bildschirm „Administrator Account Setup“ (Einrichten des Administratorkontos)

Der Bildschirm „Administrator Account Setup“ (Einrichten des Administratorkontos) zeigt am Anfang den Namen des aktiven Gehäuses sowie seine aktuellen Einstellungen an. Wenn im Bildschirm „Enclosure Selection“ (Gehäuseauswahl) mehrere Gehäuse ausgewählt wurden, wird eine Schaltfläche aktiviert, über die Sie separate Eingaben für jedes ausgewählte Onboard Administrator-Modul anzeigen können.



Feld	Möglicher Wert	Beschreibung
Full Name (Vollständiger Name)	0 bis 20 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Der vollständige Name des Benutzers
Contact (Kontakt)	0 bis 20 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Kontaktinformationen für das Benutzerkonto. Bei den Kontaktinformationen kann es sich um den Namen einer Person, eine Telefonnummer oder andere nützliche Informationen handeln.
Administrator Password (Administrator-Kennwort)	3 bis 40 Zeichen, einschließlich aller druckbaren Zeichen	Das Kennwort für das Benutzerkonto.
Administrator Password Confirm (Administrator-Kennwort bestätigen)	3 bis 40 Zeichen, einschließlich aller druckbaren Zeichen	Muss mit dem Eintrag im Feld „Administrator Password“ (Administrator-Kennwort) übereinstimmen.
Enable Insight Display PIN protection (Insight Display-PIN-Schutz aktivieren)	Aktivieren oder deaktivieren Sie das Kontrollkästchen	Aktivieren Sie das Kontrollkästchen, wenn zum Zugriff auf das Insight Display des Gehäuses die Eingabe eines PIN-Codes erforderlich sein soll.

Feld	Möglicher Wert	Beschreibung
PIN Code (PIN-Code)	1 bis 6 Zeichen aus den Zeichensätzen 0 bis 9, a bis z und A bis Z	Der PIN-Code für das Insight Display des Gehäuses.
PIN Code Confirm (PIN-Code bestätigen)	1 bis 6 Zeichen aus den Zeichensätzen 0 bis 9, a bis z und A bis Z	Muss mit dem Eintrag im Feld „Insight Display PIN“ (Insight Display-PIN) übereinstimmen.

HINWEIS: Wenn der Onboard Administrator mit der Einstellung ON/DEBUG für den FIPS-Modus betrieben wird, kann der PIN-Schutz nicht deaktiviert werden.

Bildschirm „Local User Accounts“ (Lokale Benutzerkonten)

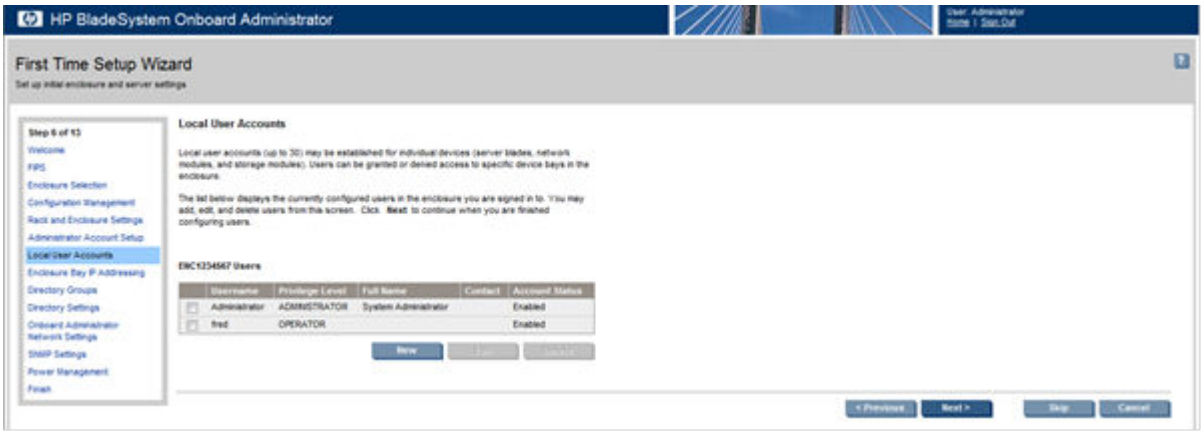
Im Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) werden die Benutzerkonten angezeigt, die dem aktiven Onboard Administrator-Modul zugewiesen wurden. Außerdem können in diesem Bildschirm Konten hinzugefügt, bearbeitet und gelöscht werden.

New (Neu): Klicken Sie auf **New** (Neu), um einen neuen Benutzer zum ausgewählten Gehäuse hinzuzufügen. Der Bildschirm „Add Local User“ (Lokalen Benutzer hinzufügen) wird angezeigt.

HINWEIS: Im FIPS-Modus OFF können maximal 30 Benutzerkonten konfiguriert werden, während im FIPS-Modus ON oder DEBUG maximal 21 Benutzerkonten konfiguriert werden können. Im maximalen Benutzerkontenlimit sind reservierte Konten enthalten, wie z. B. die Administrator- und Virtual Connect-Konten.

Edit (Bearbeiten) – Wählen Sie einen Benutzer aus (es kann nur jeweils ein Benutzer ausgewählt werden), indem Sie das Kontrollkästchen neben dem Namen des betreffenden Benutzers markieren. Klicken Sie auf **Edit** (Bearbeiten), um die Einstellungen auf dem Bildschirm „Edit Local User“ (Lokalen Benutzer bearbeiten) zu ändern.

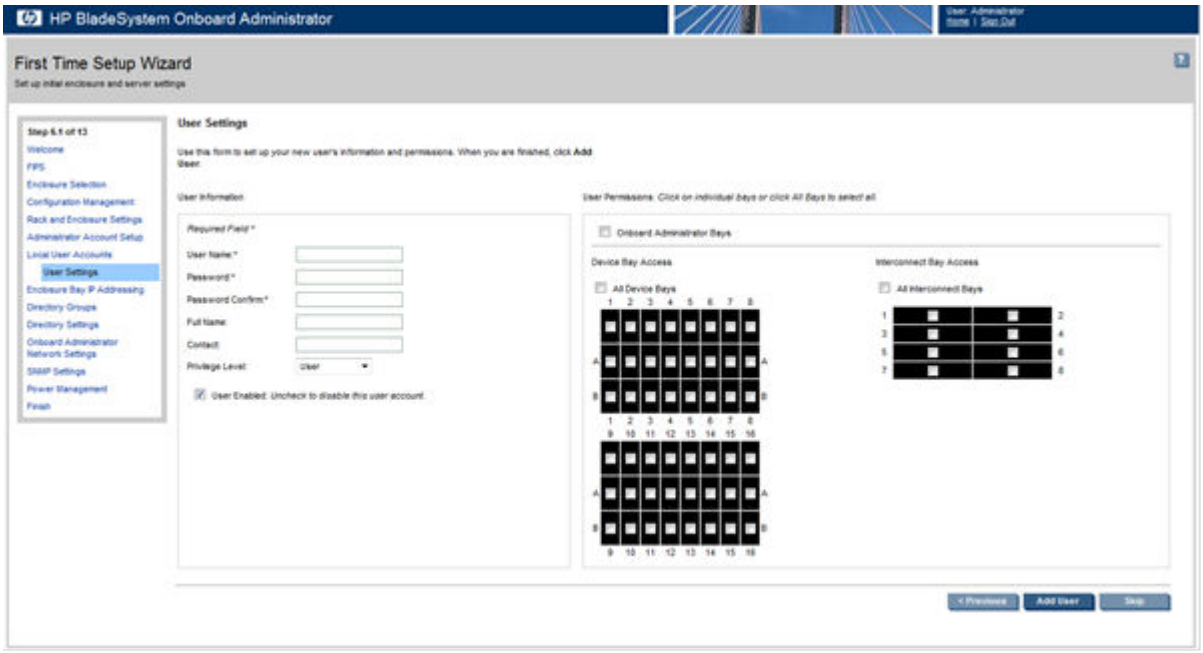
Delete (Löschen) – Wählen Sie den bzw. die zu löschenden Benutzer aus, indem Sie das Kontrollkästchen neben dem Namen der betreffenden Benutzer aktivieren. Um die Konten zu entfernen, klicken Sie auf **Delete** (Löschen). Bei dem Versuch, das letzte verbleibende Administratorkonto zu löschen, wird in einer Warnung darauf hingewiesen, dass das Administratorkonto nicht gelöscht werden kann, und der Löschvorgang wird abgebrochen.



Bildschirm „User Settings“ (Benutzereinstellungen)

Der Bildschirm „User Settings“ (Benutzereinstellungen) zeigt die konfigurierbaren Benutzerinformationen an. Geben Sie die Benutzerinformationen in den Bereichen „User Information“

(Benutzerinformationen) und „User Permissions“ (Benutzerberechtigungen) ein. Um die Informationen zu speichern, klicken Sie auf **Add User** (Benutzer hinzufügen). Klicken Sie auf **Cancel** (Abbrechen), um zum Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) zurückzukehren.



Markieren Sie für jeden hinzugefügten Benutzer die entsprechenden Kontrollkästchen, um den Zugriff auf Server und Verbindungsmoduleinschübe zu erlauben.

Mögliche Werte sowie eine Beschreibung der einzelnen Felder finden Sie unter „Hinzufügen eines lokalen Benutzers“ (Add Local User (Lokalen Benutzer hinzufügen) auf Seite 323).

Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub)

Über die „Enclosure Bay IP Addressing“ (IP-Adressierung für den Gehäuseeinschub)-Bildschirme des Assistenten für die Erstkonfiguration (First Time Setup Wizard) können feste IPv4- und IPv6-Adressen für Onboard Administrator-Gehäuseeinschübe konfiguriert werden. Mit der Onboard Administrator-EBIPA-Funktion können Sie eine feste IP-Adresse basierend auf der Einschubsnummer bereitstellen, wodurch die IP-Adresse eines bestimmten Einschubs selbst dann beibehalten wird, wenn ein Gerät ausgewechselt wird. Als Verwaltungsschnittstelle für die in den Einschüben eingesteckten Komponenten muss DHCP eingestellt werden. EBIPA kann nur verwendet werden, wenn die Geräte zum Starten über DHCP eingestellt sind. Wenn für ein Gerät die statische IP-Adressierung konfiguriert ist, muss es zum Ändern der EBIPA-IP-Adresse in DHCP manuell neu konfiguriert werden.

HINWEIS: In der Onboard Administrator-Dokumentation werden EBIPA IP-Adressen als „feste IP-Adressen“ oder „feste DHCP-Adressen“ bezeichnet. Dies bedeutet, dass jede dieser Adressen eine IP-Adresse ist, die permanent mit einer bestimmten Einschubsnummer verknüpft ist, unabhängig davon, welches Gerät derzeit tatsächlich am Einschub angeschlossen ist.

Für die iLO-Einschübe des Server Blade sowie die Verbindungsmodul-Verwaltungseinschübe können auf verschiedene Arten IP-Adressen über das Verwaltungsnetzwerk bezogen werden: über die dynamische IP-Adressierung mittels eines DHCP-Servers, die statische IP-Adressierung, SLAAC über Routerankündigungen (nur IPv6) oder EBIPA. Wenn Ihr Netzwerk über einen DHCP-Dienst verfügt oder wenn Sie statische IP-Adressen manuell für die Server Blades und Verbindungsmodule

zuweisen möchten, klicken Sie auf **Skip** (Überspringen), um das Konfigurieren der Gehäuseeinschubs-IP-Adressierung zu überspringen.

EBIPA weist feste DHCP-IP-Adressen nur der Verwaltungsschnittstelle für Server-iLOs und Verbindungsmodule zu, die sich in dem internen Verwaltungsnetzwerk des Gehäuse befinden. EBIPA weist keine IP-Adressen für andere Komponenten im Verwaltungsnetzwerk extern des Gehäuses zu und kann nicht als DHCP-Server in Produktionsnetzwerken verwendet werden.

Für das Server Blade-iLO wird standardmäßig die DHCP-Adressierung eingestellt, die über die Netzwerkverbindung des aktiven Onboard Administrator-Moduls bezogen wird. Für Verbindungsmodule, die über eine interne Management-Netzwerkverbindung zum Onboard Administrator verfügen, kann ebenfalls standardmäßig die DHCP-Adressierung gelten.

HINWEIS: EBIPA erzwingt eindeutige IP-Adressen für alle Einschübe, sogar dann, wenn sich die Einschübe auf einem anderen VLAN befinden.

EBIPA-Konfigurationsrichtlinien

Dieser Abschnitt enthält allgemeine Konfigurationsinformationen. Spezifische Konfigurationsinformationen für IPv4 oder IPv6 finden Sie in den entsprechenden nachfolgenden Abschnitten.

Wenn Ihre Einrichtung die Zuweisung fester IP-Adressen bevorzugt, können Sie für die einzelnen Server Blade-iLO-Einschübe und Verbindungsmodul-Management-Einschübe eindeutige feste Adressen angeben oder einzelnen Server Blade- und Verbindungsmoduleinschüben über EBIPA einen Bereich fester IP-Adressen zuweisen. Wenn feste Adressen einzeln angegeben werden, können Subnetzmaske (IPv4), Gateway, DNS-Server, NTP-Server (IPv4-Verbindungsmodul) und Domänenname für jeden einzelnen Einschub gleich oder verschieden sein. Wenn über EBIPA ein Bereich fester Adressen zugewiesen wird, müssen Sie die erste IP-Adresse in einem Bereich und die Subnetzmaske angeben. Wenn Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen) für den betreffenden Einschub klicken, werden den unterhalb dieses Einschubs aufgelisteten Einschüben automatisch aufeinander folgende IP-Adressen zugewiesen. Die Angaben für Subnetzmaske, Gateway, DNS-Server, NTP-Server und Domänenname werden ebenfalls auf die einzelnen aufeinander folgenden Einschübe in der Liste kopiert.

Wenn Sie beispielsweise für EBIPA-Einschub 1 die IPv4-Adresse 16.100.226.21 angeben, dann werden den Einschüben 1 bis 16 mit der Funktion Autofill (Autom. ausfüllen) aufeinander folgende IP-Adressen im Bereich 16.100.226.21 bis 16.100.226.36 zugewiesen. Wenn Sie beispielsweise für Verbindungsmoduleinschub 3 16.200.139.51 angeben und die Funktion verwenden, dann werden den Verbindungsmoduleinschüben 3 bis 8 aufeinander folgende IP-Adressen im Bereich 16.200.139.51 bis 16.200.139.56 zugewiesen.

HINWEIS: Mittels der Schaltfläche **Autofill** (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt.

Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske oder ein IPv6-Subnetzpräfix an, die bzw. das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske oder eines Präfix, die bzw. das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.

Wenn Sie feste IP-Adressen für Managementprozessoren verwenden, dann können Sie mit dem Onboard Administrator-Befehl `hponcfg` das RIBCL-Skript mit den iLO-Netzwerkeinstellungen an ein iLO senden, sofern dieses iLO bereits eine IP-Adresse besitzt. EBIPA kann verwendet werden, um IP-Adressen auf iLOs zu laden, so dass mit dem Onboard Administrator-Befehl `hponcfg`

Konfigurationsskripte an diese iLOs gesendet werden können. Änderungen an den iLO-Netzwerkeinstellungen führen dazu, dass dieses iLO die Netzwerkschnittstelle zurücksetzt und die aktuellen Verbindungen für einige Sekunden unterbricht.

Bei Server Blades doppelter Dichte dürfen für die Basiseinschübe (Einschub 1, 2 usw.) keine EBIPA-Einstellungen konfiguriert werden. Konfigurieren Sie die Einschübe der Seite A (1A, 2A usw.) und die Einschübe der Seite B (1B, 2B usw.). Mit der Funktion Autofill (Autom. ausfüllen) werden den Einschüben, die unterhalb des Einschubs aufgelistet werden, für den Sie die erste IP-Adresse im Bereich angeben, aufeinander folgende IP-Adressen zugewiesen (wenn Sie z. B. die IP-Adresse für Einschub 1A angeben und die Funktion Autofill (Autom. ausfüllen) anwenden, dann werden den Einschüben 2A, 3A usw. aufeinander folgende Adressen zugewiesen).

Verwenden Sie zum Konfigurieren der Verbindungsmoduleinschübe „Interconnect List“ (die Verbindungsmodulliste unterhalb von „Device List“ (Geräteliste) auf dem gleichen Assistenten-Bildschirm).

Um die Einstellungen zu übernehmen, klicken Sie auf **Next** (Weiter).

Die Server in den Geräteeinschüben rufen die Geräteeinschubs-EBIPA-Adressen innerhalb weniger Minuten automatisch ab. Die Verbindungsmodul-Switch-Module müssen jedoch manuell neu gestartet werden. Klicken Sie dazu auf jeder Onboard Administrator-Verbindungsmodul-Informationsseite auf die Schaltfläche **Virtual Power** (Virtueller Netzschalter).

Einrichten des Gehäuses mittels EBIPA ohne aktive Netzwerkverbindung

1. Konfigurieren Sie mit Insight Display eine statische IP für Onboard Administrator. Im Bildschirm „Enclosure Info“ (Gehäuse-Info) des Insight Display wird die Service-IP-Adresse des aktiven OA angezeigt. Schließen Sie den Client-PC an den Gehäuse-Service-Port (Gehäuse-Link-up-Anschluss) zwischen den OA-Einschüben mit einem Standard-Ethernet-Patch-Kabel an. Die Client-PC-NIC muss für DHCP konfiguriert sein, da er ungefähr 1 Minute später eine IP-Adresse im Bereich 169.254.x.y abruft.
2. Starten Sie einen Web-Browser (oder alternativ eine Telnet- oder SSH-Sitzung), und wählen Sie die Onboard Administrator-Service-IP-Adresse aus, die auf dem Insight Display des Gehäuses im Bildschirm „Enclosure Info“ (Gehäuse-Info) angezeigt wird.
3. Melden Sie sich mit dem am aktiven Onboard Administrator-Modul angebrachten administrativen Kennwort als Administrator bei Onboard Administrator an.
4. Aktivieren Sie im Assistenten für die Erstkonfiguration (First Time Setup Wizard) die Geräteeinschubs-EBIPA mit einer anfänglichen festen IP-Adresse, und aktivieren Sie die Verbindungsmoduleinschubs-EBIPA mit einer anderen anfänglichen IP-Adresse. Nachdem der Assistent für die Erstkonfiguration ausgeführt wurde, können Sie die EBIPA-Einstellungen jederzeit durch Auswahl von **Enclosure Bay IP Addressing** (Gehäuseeinschubs-IP-Adressierung) in der Liste „Enclosure Settings“ (Gehäuseeinstellungen) ändern.

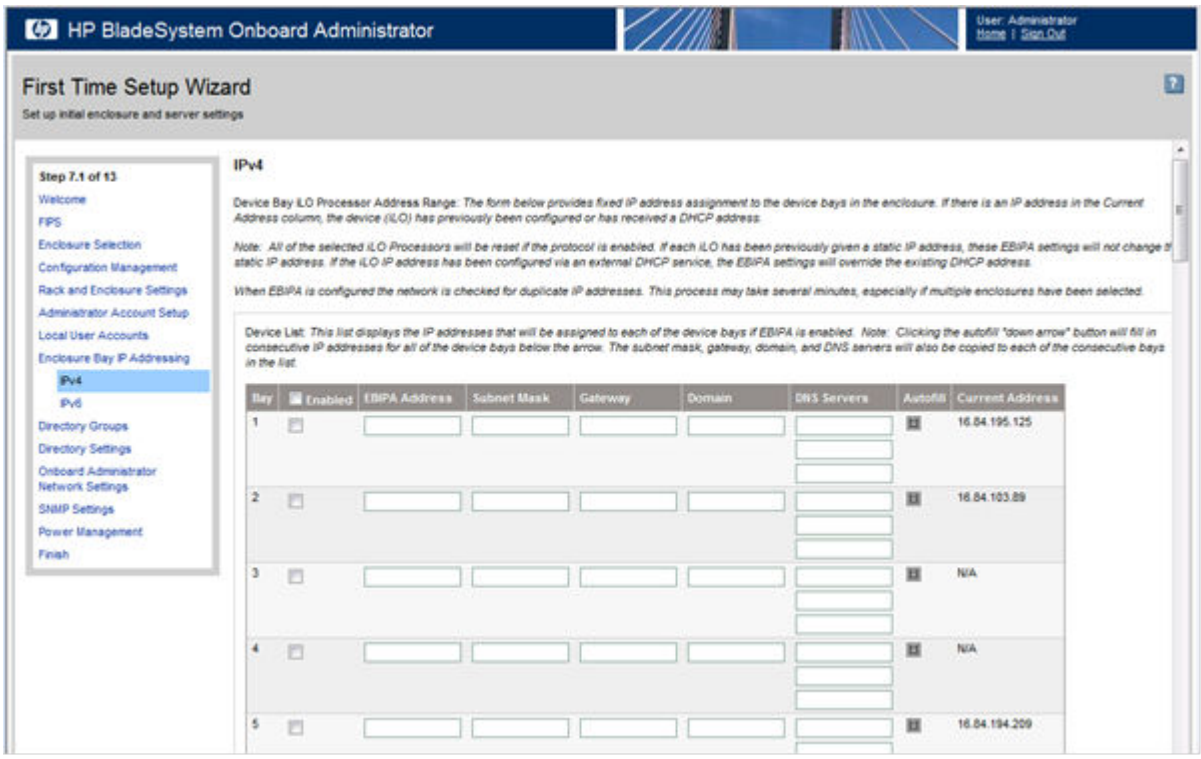
   Durch Klicken auf die Schaltfläche **Autofill** (Autom. ausfüllen) werden so viele sequenzielle, feste IP-Adressen erstellt wie erforderlich. Die Angaben für Subnetzmaske, Gateway, DNS-Server, NTP-Server und Domänenname werden ebenfalls auf die einzelnen aufeinander folgenden Einschübe in der Liste kopiert. Alternativ dazu können Sie einzelne IP-Adressen zuweisen, indem Sie die gewünschte IP-Adresse manuell in das Feld „EBIPA Address“ (EBIPA-Adresse) für den betreffenden Einschub eingeben. Die Werte für Subnetzmaske, Gateway, DNS-Server, NTP-Server und Domäne können bei jedem einzelnen Einschub gleich oder verschieden sein.

   Nachdem die Einstellungen übernommen wurden, rufen die Server in den Geräteeinschüben die Geräteeinschubs-EBIPA-Adressen innerhalb weniger Minuten automatisch ab. Die Verbindungsmodul-Switch-Module müssen jedoch manuell neu gestartet werden. Klicken Sie

dazu auf jeder Onboard Administrator-Verbindungsmodul-Informationsseite auf die Schaltfläche **Virtual Power** (Virtueller Netzschalter).

5. Überprüfen Sie anhand der Onboard Administrator-Komponentenliste, ob die Server Blade-iLO-Adressen gemäß der anfänglichen EBIPA-IP-Adresse und dem entsprechenden Bereich eingerichtet wurden.

EBIPA-IPv4-Bildschirms des Assistenten für die Erstkonfiguration


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
First Time Setup Wizard
Set up initial enclosure and server settings
Step 7.1 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
Enclosure Bay IP Addressing
IPv4
IPv6
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
IPv4
Device Bay iLO Processor Address Range: The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change it static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.
When EBIPA is configured the network is checked for duplicate IP addresses. This process may take several minutes, especially if multiple enclosures have been selected.
Device List: This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Subnet Mask
Gateway
Domain
DNS Servers
Autofill
Current Address
1
16.84.195.125
2
16.84.193.89
3
N/A
4
N/A
5
16.84.194.209

HINWEIS: Verwenden Sie beim Konfigurieren von EBIPA-zugewiesenen Adressen nicht den Bereich 169.254.x.x, da dieser Netzwerkadressbereich für den Onboard Administrator reserviert ist.

Komponentenliste

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse der Komponente.
Enabled (Aktiviert)	Aktiviert EBIPA-Einstellungen für den Geräteeinschub. Durch Auswahl des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-Einstellungen für alle Geräteeinschübe aktiviert werden. Durch Auswahl des jeweiligen Kontrollkästchens für einzelne Geräteeinschübe kann der betreffende Geräteeinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste IP-Adresse, die Sie dem Geräteeinschub zuweisen möchten. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Subnet Mask (Subnetzmaske)	Subnetzmaske für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Gateway	Die feste Gateway-IP-Adresse, die Sie den Geräteeinschüben zuweisen möchten. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).

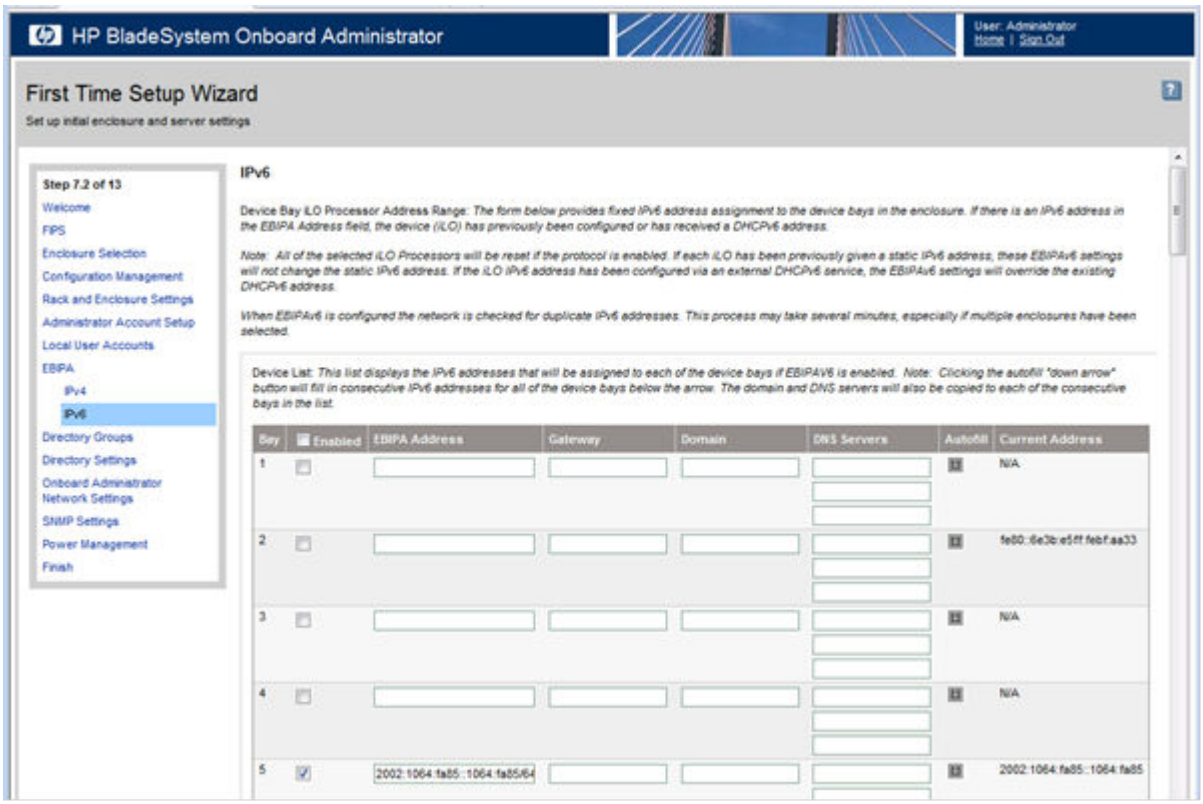
Spalte	Beschreibung
DNS Servers (DNS-Server)	IP-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Autofill (Autom. ausfüllen)	Weist den unten in der Komponentenliste ausgewählten Geräteeinschüben aufeinanderfolgende IP-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske an, die ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske, die diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IP-Adresse des Geräteeinschubs.

Verbindungsmodulliste

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Verbindungsmoduls.
Enabled (Aktiviert)	Aktiviert EBIPA-für-IPv4-Einstellungen für den Verbindungsmoduleinschub. EBIPA-für-IPv4-Einstellungen für alle Verbindungsmoduleinschübe können durch Markierung des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile aktiviert werden. Durch die Markierung des jeweiligen Kontrollkästchens für einzelne Verbindungsmoduleinschübe kann der betreffende Verbindungsmoduleinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste DHCP-IP-Adresse, die Sie dem Geräteeinschub zuweisen möchten.
Subnet Mask (Subnetzmaske)	Subnetzmaske für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Gateway	Gateway-Adresse für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv4-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
NTP Server (NTP-Server)	Die IPv4-Adresse des primären Servers, die für die Synchronisierung von Uhrzeit und Datum über das NTP-Protokoll verwendet wird ###.###.###.###, wobei ### im Bereich zwischen 0 und 255 liegt.
Autofill (Autom. ausfüllen)	Weist den unten in der Verbindungsmodulliste ausgewählten Verbindungsmoduleinschüben aufeinanderfolgende IPv4-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die

Spalte	Beschreibung
	Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske an, die ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske, die diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv4-Adresse des Verbindungsmoduleinschubs.

EBIPA-IPv6-Bildschirm des Assistenten für die Erstkonfiguration


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
First Time Setup Wizard
Set up initial enclosure and server settings
Step 7.2 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
EBIPA
IPv4
IPv6
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
IPv6
Device Bay iLO Processor Address Range: The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.
When EBIPAv6 is configured the network is checked for duplicate IPv6 addresses. This process may take several minutes, especially if multiple enclosures have been selected.
Device List: This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
N/A
2
fe80::6e3b:e5ff:febf:aa33
3
N/A
4
N/A
5
2002:1064:fa85::1064:fa85/64
2002:1064:fa85::1064:fa85

HINWEIS: Verwenden Sie beim Konfigurieren von EBIPA-zugewiesenen Adressen nicht das Präfix fe80::/10, da dieses Netzwerkpräfix für verbindungslokale SLAAC-Adressen reserviert ist.

HINWEIS: Damit feste EBIPA-IPv6-Adressen erfolgreich konfiguriert werden, muss die Einstellung **Enable IPv6** (IPv6 aktivieren) aktiviert sein. Sie können diese Einstellung über den Bildschirm „Network IPv6 Settings“ (Netzwerk-IPv6-Einstellungen) im „First Time Setup Wizard“ (Assistent der Erstkonfiguration) aktivieren.

Die Einstellungen **Enable SLAAC** (SLAAC aktivieren) und **Enable DHCPv6** (DHCPv6 aktivieren) wirken sich nicht auf die EBIPA-IPv6-Funktionalität aus.

Komponentenliste

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Komponente.
Enabled (Aktiviert)	Aktiviert EBIPA-Einstellungen für den Geräteeinschub. Durch Auswahl des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-Einstellungen für alle Geräteeinschübe aktiviert werden. Durch Auswahl des jeweiligen Kontrollkästchens für einzelne Geräteeinschübe kann der betreffende Geräteeinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste IPv6-Adresse, die Sie dem Geräteeinschub zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Das Präfix /### reicht von 1 bis 128; die Präfixlänge ist vorgeschrieben.
Gateway	Die feste IPv6-Gateway-Adresse, die Sie den Geräteeinschüben zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Geben Sie kein Präfix an. Es wird vorausgesetzt, dass das Gateway innerhalb des Netzwerks erreichbar ist. Wenn dieses Gateway als verbindungslokale Adresse angegeben wird, wird das Gateway immer auf dem Gehäusegerät konfiguriert, das von dieser Adresse Gebrauch macht. Wenn das Gateway mit irgendeiner anderen Art von IPv6-Adresse angegeben wird, sendet Onboard Administrator zum Identifizieren der verbindungslokalen Adresse des Gateway-Geräts, das beim Konfigurieren der Gehäusekomponenten verwendet werden soll, Nachbaranfrageaufforderungen. Wenn das Gateway nicht vorhanden ist oder nicht auf die Nachbaranfrageaufforderungen reagiert, wird kein Gateway konfiguriert.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv6-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
Autofill (Autom. ausfüllen)	Weist den unten in der Komponentenliste ausgewählten Geräteeinschüben aufeinanderfolgende IPv6-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) ein IPv6-Subnetzpräfix an, das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe eines Präfix, das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv6-Adresse des Geräteeinschubs.

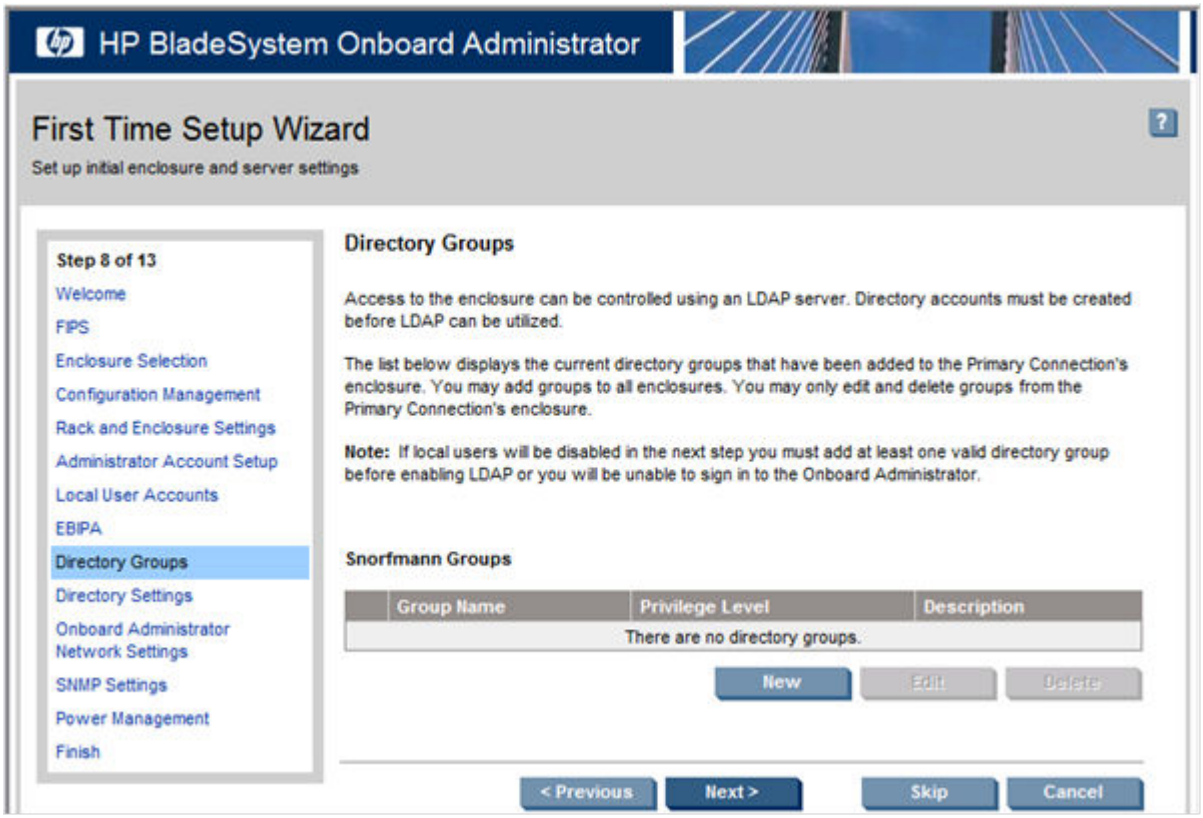
Verbindungsmodulliste

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Verbindungsmoduls.
Enabled (Aktiviert)	Aktiviert EBIPA-für-IPv6-Einstellungen für den Verbindungsmoduleinschub. Durch Markierung des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-für-IPv6-Einstellungen für alle Verbindungsmoduleinschübe aktiviert werden. Durch Markierung des jeweiligen Kontrollkästchens für einzelne Verbindungsmoduleinschübe kann der betreffende Verbindungsmoduleinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste DHCP-IPv6-Adresse, die Sie dem Verbindungsmoduleinschub zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Das Präfix /### reicht von 1 bis 128; die Präfixlänge ist vorgeschrieben.
Gateway	Die feste Gateway-IPv6-Adresse, die Sie den Verbindungsmoduleinschüben zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Geben Sie kein Präfix an. Es wird vorausgesetzt, dass das Gateway innerhalb des Netzwerks erreichbar ist. Wenn dieses Gateway als verbindungslokale Adresse angegeben wird, wird das Gateway immer auf dem Gehäusegerät konfiguriert, das von dieser Adresse Gebrauch macht. Wenn das Gateway mit irgendeiner anderen Art von IPv6-Adresse angegeben wird, sendet Onboard Administrator zum Identifizieren der verbindungslokalen Adresse des Gateway-Geräts, das beim Konfigurieren der Gehäusekomponenten verwendet werden soll, Nachbaranfrageaufforderungen. Wenn das Gateway nicht vorhanden ist oder nicht auf die Nachbaranfrageaufforderungen reagiert, wird kein Gateway konfiguriert.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv6-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
Autofill (Autom. ausfüllen)	Weist den unten in der Verbindungsmodulliste ausgewählten Verbindungsmoduleinschüben aufeinanderfolgende IPv6-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) ein IPv6-Subnetzpräfix an, das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe eines Präfix, das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv6-Adresse des Verbindungsmduleinschubs.

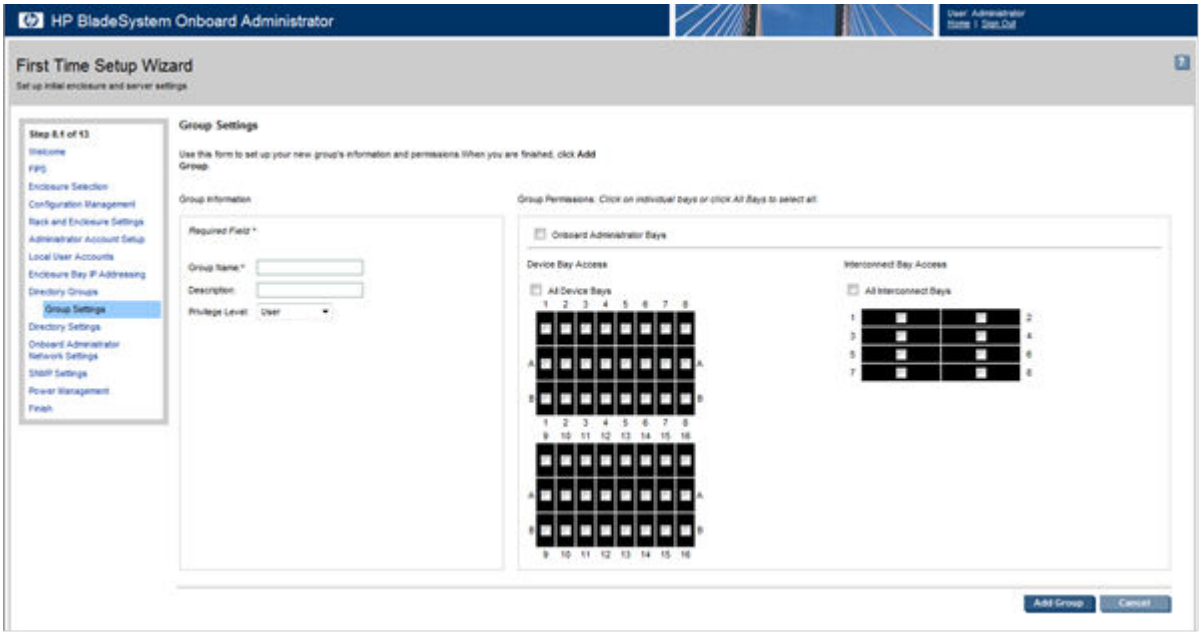
Bildschirm „Directory Groups Configuration“ (Konfiguration von Verzeichnisgruppen)

LDAP ist ein offenes Protokoll für den Zugriff auf Informationsverzeichnisse. Obwohl LDAP auf dem X.500-Standard basiert, ist LDAP weniger komplex. LDAP unterstützt TCP/IP, so dass Anwendungen unabhängig von dem Server arbeiten können, auf dem sich das Verzeichnis befindet.

Die folgende Abbildung zeigt den Bildschirm „Directory Groups“ (Verzeichnisgruppen) des Assistenten für die Erstkonfiguration (First Time Setup Wizard), auf dem Sie Verzeichnisgruppen hinzufügen, bearbeiten und löschen können:


HP BladeSystem Onboard Administrator
First Time Setup Wizard
Set up initial enclosure and server settings
Step 8 of 13
Welcome
FIPS
Enclosure Selection
Configuration Management
Rack and Enclosure Settings
Administrator Account Setup
Local User Accounts
EBIPA
Directory Groups
Directory Settings
Onboard Administrator Network Settings
SNMP Settings
Power Management
Finish
Directory Groups
Access to the enclosure can be controlled using an LDAP server. Directory accounts must be created before LDAP can be utilized.
The list below displays the current directory groups that have been added to the Primary Connection's enclosure. You may add groups to all enclosures. You may only edit and delete groups from the Primary Connection's enclosure.
Note: If local users will be disabled in the next step you must add at least one valid directory group before enabling LDAP or you will be unable to sign in to the Onboard Administrator.
Snorfmann Groups
Group Name
Privilege Level
Description
There are no directory groups.
New
Edit
Delete
< Previous
Next >
Skip
Cancel

Um eine Verzeichnisgruppe hinzuzufügen, klicken Sie auf **New** (Neu). Die folgende Abbildung zeigt den Bildschirm „Group Settings“ (Gruppeneinstellungen) des Assistenten für die Erstkonfiguration (First Time Setup Wizard), auf dem Sie eine neue Verzeichnisgruppe konfigurieren und Verzeichniszugriff für die ausgewählten Gehäuse festlegen können.



Der Zugriff auf das Gehäuse kann über LDAP gewährt werden. Zur Verwendung des LDAP-Servers müssen Sie Verzeichniskonten erstellen.

Der Bildschirm „Directory Groups“ (Verzeichnisgruppen) zeigt die Verzeichnisgruppen an, die zum Gehäuse „Primary Connection“ (Hauptverbindung) hinzugefügt wurden. Sie können allen Gehäusen Benutzergruppen hinzufügen. Sie können Benutzergruppen nur im Gehäuse „Primary Connection“ (Primäre Verbindung) bearbeiten und löschen. Zur Verwendung von LDAP-Diensten müssen Sie mindestens eine Verzeichnisgruppe hinzufügen.

Spalte	Beschreibung
Kontrollkästchen	Dient zur Auswahl der Verzeichnisgruppe zum Bearbeiten oder Löschen.
Group Name (Gruppenname)	1 bis 255 Zeichen und enthält die gleichen Zeichen wie Suchkontexte. Der Gruppenname dient zur Ermittlung der Gruppenmitgliedschaft von LDAP-Benutzern. Der Gruppenname muss einer der folgenden fünf Eigenschaften einer Verzeichnisgruppe entsprechen: „Name“ (Name), „Distinguished Name“ (Eindeutiger Name), „Common Name“ (Allgemeiner Name), „Display Name“ (Anzeigename) oder „SAM Account Name“ (SAM-Konto-Name). Bei verschachtelten Gruppen basiert die Entsprechung auf `objectSid` (einem Attribut, durch das die Sicherheits-ID der Gruppe angegeben wird). Der eindeutige Name wird empfohlen, um die LDAP-Gruppe eindeutig zu bezeichnen. Wenn das Onboard Administrator-Modul für die Suche im GC-Port konfiguriert ist und kein eindeutiger Name verwendet wird, führt dies möglicherweise zu nicht korrekten Entsprechungen in verschiedenen Domänen und einer nicht beabsichtigen Autorisierung.
Privilege Level (Berechtigungsebene)	Bestimmt, welche Verwaltungsfunktionen der Benutzer ausführen darf. Als Benutzerberechtigungsebene kommen Administrator, Operator (Bediener) oder User (Benutzer) in Frage.
Description (Beschreibung)	0 bis 58 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen Die Beschreibung der LDAP-Gruppe, eine lesbarere Version des Gruppennamens oder andere nützliche Informationen.

- **New** (Neu): Klicken Sie auf **New** (Neu), um zum ausgewählten Gehäuse eine neue Verzeichnisgruppe hinzuzufügen. Sie können maximal 30 Verzeichnisgruppen hinzufügen. Der Bildschirm „Add LDAP Group“ (LDAP-Gruppe hinzufügen) wird angezeigt.
- **Edit** (Bearbeiten) – Wählen Sie eine Verzeichnisgruppe aus, die bearbeitet werden soll, indem Sie das Kontrollkästchen neben dem Namen der Gruppe aktivieren. Klicken Sie auf **Edit** (Bearbeiten), um die Einstellungen auf dem Bildschirm „Edit LDAP Group“ (LDAP-Gruppe bearbeiten) zu ändern.
- **Delete** (Löschen) – Wählen Sie eine Verzeichnisgruppe aus, die gelöscht werden soll, indem Sie das Kontrollkästchen neben dem Namen der Gruppe aktivieren. Um die Gruppe zu entfernen, klicken Sie auf **Delete** (Löschen).

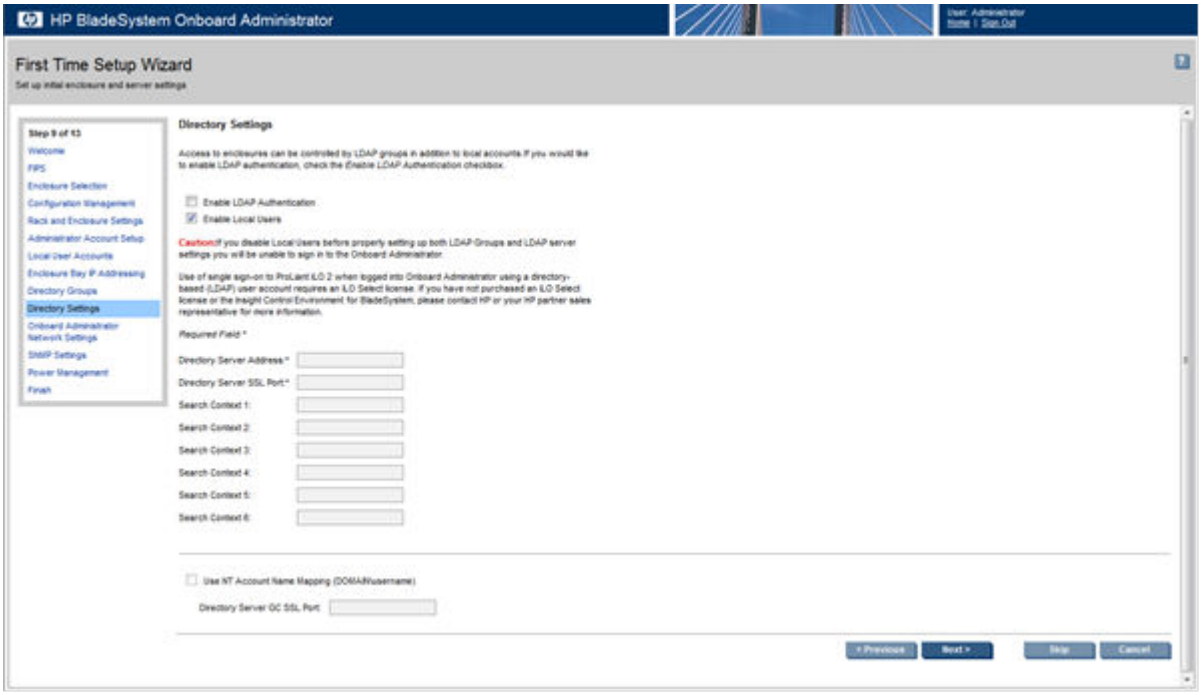
Unterstützung verschachtelter LDAP-Gruppen

Bei Verwendung von Microsoft Active Directory können Sie eine oder mehrere Gruppen in einer anderen Gruppe platzieren. Gruppen, die in einer anderen Gruppe enthalten sind, werden als verschachtelte Gruppen bezeichnet. Die Gruppe, in der sich die verschachtelten Gruppen befinden, wird als Verschachtelungsgruppe bezeichnet. Verschachtelte Gruppen bieten den Vorteil, dass sich Benutzer einer verschachtelten Gruppe bei Onboard Administrator anmelden können, sofern deren Verschachtelungsgruppe entsprechend konfiguriert ist. Angenommen, `group2` ist innerhalb von `group1` verschachtelt. Benutzer in `group2` dürfen sich bei dem Onboard Administrator anmelden, sofern die übergeordnete LDAP-Gruppe (`group1`) dem Onboard Administrator hinzugefügt wird und über einen der Suchkontexte auffindbar ist. Der Suchkontext ist nicht auf die genaue Position eingeschränkt: Wenn sich der Suchkontextpfad auf einer oberen Ebene der LDAP-Verzeichnisstruktur befindet, wird die untergeordnete Verzeichnisstruktur durchsucht. Der Onboard Administrator unterstützt nur den Sicherheitsgruppentyp. Der Verteilungsgruppentyp wird nicht unterstützt.

Um die Einstellungen zu übernehmen, klicken Sie auf **Next** (Weiter).

Bildschirm „Directory Settings“ (Verzeichniseinstellungen)

Verwenden Sie den folgenden Bilschirm „Directory Settings“ (Verzeichniseinstellungen), um den Verzeichniszugriff für die derzeit ausgewählten Gehäuse festzulegen.



HINWEIS: Die LDAP-Funktion von Onboard Administrator unterstützt Microsoft® Active Directory mittels des Attributs `memberOf`. Mittels des Attributs `groupMembership` wird auch Novell eDirectory unterstützt. OpenLDAP is not supported.

Auf diesem Bildschirm können Sie die folgenden Einstellungen konfigurieren:

- **Enable LDAP Authentication** (LDAP-Authentifizierung aktivieren) – Markieren Sie dieses Kontrollkästchen, um die Authentifizierung einer Benutzeranmeldung durch einen Verzeichnisserver zu veranlassen.
- **Enable Local Users** (Lokale Benutzer aktivieren) – Markieren Sie dieses Kontrollkästchen, um die Benutzeranmeldung mit einem lokalen Benutzerkonto anstelle eines Verzeichniskontos zu ermöglichen.
- **Search Context** (Suchkontext) – Geben Sie einen bis sechs Suchkontexte an. Ein Suchkontext ist ein Suchfilter oder eine Verknüpfung mit einem gemeinsamen Verzeichnis, durch den definiert wird, dass der Benutzer mit der Verzeichnissuche am angegebenen Pfad beginnen soll. Durch Angabe eines Suchkontexts müssen Benutzer bei der Anmeldung nicht ihre vollständigen DNs angeben. DNs können lang sein, und Benutzer kennen möglicherweise ihre DN nicht oder besitzen möglicherweise Konten in verschiedenen Verzeichniskontexten. Der Onboard Administrator versucht, den Verzeichnisdienst nach DN zu kontaktieren, und wendet dann der Reihe nach die Suchkontexte an. Dabei wird mit `Search Context 1` (Suchkontext 1) begonnen und mit allen darauf folgenden Suchkontexten fortgefahren, bis die Suche erfolgreich ist.
  - **Beispiel 1**:

    Angenommen, Sie sind `user1`. Wenn Sie als Suchkontext `ou=OU1,dc=hp,dc=com` eingeben, können Sie sich anstatt mit `cn=user1,ou=OU1,dc=hp,dc=com` mit `user1` anmelden.
  - **Beispiel 2**:

    Angenommen, die folgenden Suchkontexte sind definiert:

- Suchkontext 1: `ou=OU1,dc=hp,dc=com`
- Suchkontext 2: `ou=OU2,ou=OU1,dc=hp,dc=com`

Wenn zwei Benutzer in beiden Suchkontexten den gleichen Namen `user1` besitzen und ihre Kennwörter gleich sind, dann kontaktiert Onboard Administrator bei der versuchten Anmeldung eines der beiden Benutzer immer `cn=user1,ou=OU1,dc=hp,dc=com`.

Wenn ihre Kennwörter verschieden sind und das Kennwort für den Benutzer in `OU2` bereitgestellt wird, dann wird der von Onboard Administrator verwendete DN `cn=user1,ou=OU1,dc=hp,dc=com` zurückgewiesen, da das Kennwort nicht übereinstimmt. Bei dem nächsten Anmeldeversuch wird `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com` verwendet und er ist erfolgreich.

Der Suchkontext trifft auch auf LDAP-Verzeichnisgruppen zu, die bei der Konfiguration von verschachtelten LDAP-Gruppen hilfreich sind. Wenn der Suchkontext für eine LDAP-Verzeichnisgruppe angegeben wird, ist der genaue Kontext nicht erforderlich. Beispiel: Wenn die Position einer Gruppe ou=OU2,ou=OU1,dc=hp,dc=com ist, kann zum Auffinden diese Gruppe der Suchkontext auf höherer Ebene verwendet werden. Mit dieser Funktion lässt sich die Längenbeschränkung von Suchkontexten umgehen. Weitere Informationen zu verschachtelten Gruppen finden Sie unter „Bildschirm ‚Directory Groups Configuration' (Konfiguration von Verzeichnisgruppen)" (Bildschirm „Directory Groups Configuration" (Konfiguration von Verzeichnisgruppen) auf Seite 74).

Feld	Möglicher Wert	Beschreibung
Directory Server Address (Verzeichnisserveradresse)	IPv4 Address (IPv4-Adresse) ###.###.###.###, wobei ### den Bereich von 0 bis 255 umfasst oder den DNS-Namen des Verzeichnisservers oder den Namen der Domäne angibt. IPv6-Adresse: ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.	Die IP-Adresse, der DNS-Name oder der Name der Domäne des Verzeichnisdienstes. Ein Eintrag in diesem Feld ist erforderlich.
Directory Server SSL Port (LDAP-Port des Verzeichnisservers)	1 bis 65535	Der Port, der für die LDAP-Kommunikation verwendet wird. Port 636 ist der Standard-SSL-LDAP-Port. Ein Eintrag in diesem Feld ist erforderlich.
Search Context 1 (Suchkontext 1)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der erste durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 2 (Suchkontext 2)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der zweite durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.

Feld	Möglicher Wert	Beschreibung
Search Context 3 (Suchkontext 3)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der dritte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 4 (Suchkontext 4)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der vierte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 5 (Suchkontext 5)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der fünfte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 6 (Suchkontext 6)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der sechste durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.

- **Use NT Account Name Mapping (DOMAIN\username)** (NT-Kontonamenszuordnung verwenden (DOMÄNE\Benutzername)) – Markieren Sie dieses Kontrollkästchen, um die NT-Namenszuordnung zu aktivieren. Dieses Feld ermöglicht Benutzern die Anmeldung im NT-Format `domain\username`. Das Onboard Administrator-Modul kann optional für die Suche im globalen Verzeichnisserverkatalog konfiguriert werden, um die Informationen zum authentifizierten Benutzer und die entsprechenden berechtigten Gruppen zu suchen. Der standardmäßige GC SSL-Port für den Verzeichnisserver ist 3269. Dieses Feld ist optional. Wenn es nicht ausgefüllt wird, wird der globale Katalog nicht verwendet.

HINWEIS: Wenn die NT-Kontonamenszuordnung mit dem globalen Katalog verwendet und der Suchkontext nicht genügend eingeschränkt oder der Domänenname nicht angegeben wird, verknüpft das Onboard Administrator-Modul den authentifizierten Benutzer möglicherweise mit einem Benutzerkonto mit dem gleichen Namen in einer anderen Domäne. Der authentifizierte Benutzer würde dann die Autorisierung des Benutzers in der anderen Domäne erhalten. Wählen Sie Suchkontexte aus oder geben Sie den Domänennamen an, um Mehrdeutigkeiten bei der Anmeldung von LDAP-Benutzern zu vermeiden.

HINWEIS: Wenn die NT-Kontonamenszuordnung mit dem globalen Katalog verwendet wird und nicht zu einem einzelnen Benutzer aufgelöst werden kann, ist der Benutzer nicht für den Zugriff auf das Onboard Administrator-Modul berechtigt. Dies kann im Fall von Suchkontexten eintreten, die nicht genügend eingeschränkt wurden, wenn in verschiedenen Domänen mehrere Konten mit dem gleichen Namen vorhanden sind. Wählen Sie Suchkontexte aus, um Mehrdeutigkeiten zu vermeiden.

HINWEIS: Die auf LDAP-Servern erzwungenen Kennwortregeln unterscheiden sich möglicherweise von den für lokale Benutzerkonten erzwungenen Kennwortregeln. Stellen Sie sicher, dass beide Regelsätze den Sicherheitsrichtlinien entsprechen.

Um die Einstellungen zu übernehmen, klicken Sie auf **Next** (Weiter).

Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen)

Onboard Administrator Network Settings (Onboard Administrator-Netzwerkeinstellungen)

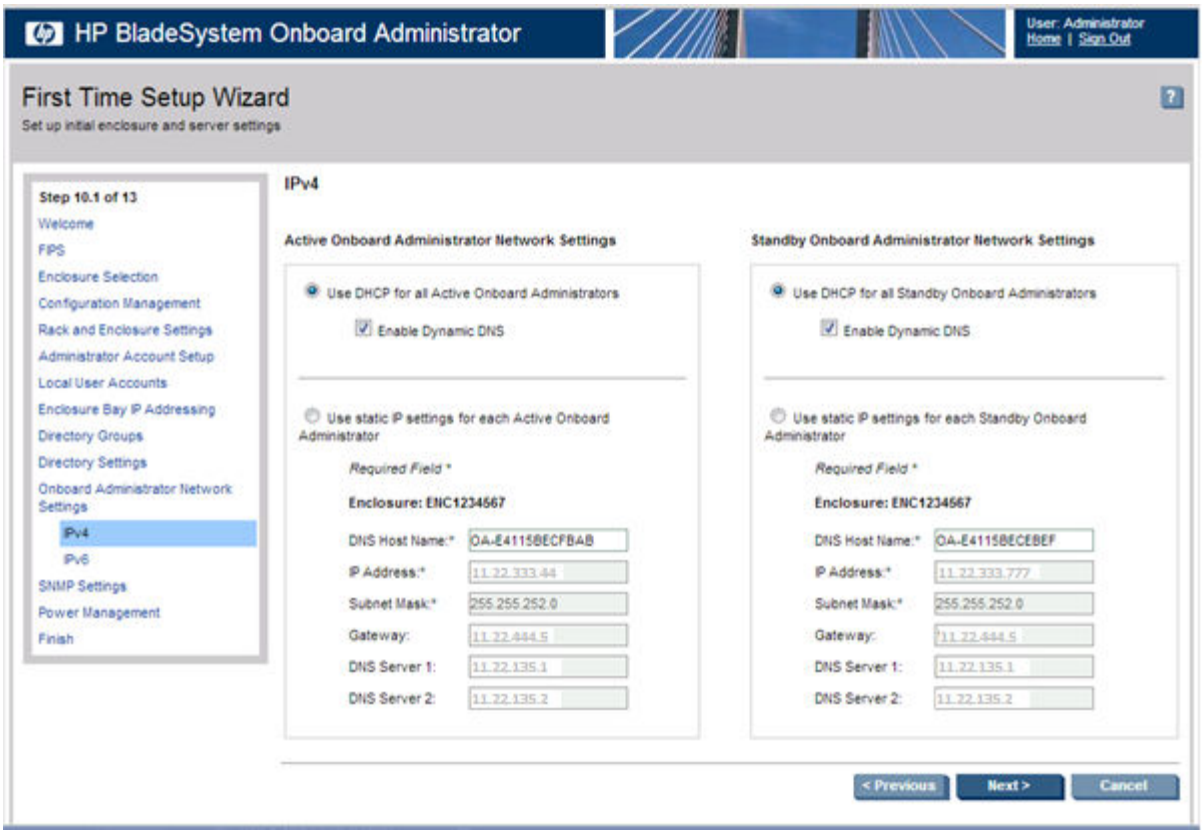
Auf den Bildschirmen „Onboard Administrator Network Settings IPv4“ (Onboard Administrator-Netzwerkeinstellungen IPv4) oder „Onboard Administrator Network Settings IPv6“ (Onboard Administrator-Netzwerkeinstellungen IPv6) können Sie die Netzwerkeinstellungen für alle Onboard Administrator-Module in den ausgewählten Gehäusen ändern. Jeder Bildschirm ermöglicht die Konfiguration der Netzwerkeinstellungen für den aktiven Onboard Administrator und den Standby-Onboard Administrator. Die Einstellungen für Onboard Administrator-Module werden nur angezeigt, wenn die Module vorhanden sind.

Bei einer Änderung der Netzwerkeinstellungen auf dem Onboard Administrator, bei dem Sie angemeldet sind, wird Ihre Verbindung mit dem Onboard Administrator möglicherweise getrennt. In diesem Fall müssen Sie sich nach dem Übernehmen der Einstellungen wieder bei dem Onboard Administrator anmelden.

Klicken Sie zum Fortfahren auf **Next** (Weiter).

Wenn Sie nicht möchten, dass die Netzwerkeinstellungen geändert werden, klicken Sie auf **Skip** (Überspringen).

Bildschirm des Assistenten für die Erstkonfiguration (First Time Setup Wizard) für die IPv4-Netzwerkeinstellungen



IPv4-Netzwerkeinstellungen des Assistenten für die Erstkonfiguration (First Time Setup Wizard)

In Onboard Administrator kann die IPv4-Netzwerkkonfiguration entweder auf dynamisch zugewiesenen IP-Adressen basieren, die von einem DHCP-Server bezogen wurden, oder auf statischen IP-Adressen, die von Ihnen manuell angegeben wurden. Sie wählen die Grundlagen für die Netzwerkkonfiguration aus, indem Sie das entsprechende Optionsfeld aktivieren. Bei Wahl von DHCP kann „Dynamic DNS“ (Dynamisches DNS) aktiviert werden.

- **Use DHCP for all Active (or Standby) Onboard Administrator** (DHCP für alle aktiven (oder Standby-) Onboard Administrator verwenden) – Bezieht die IP-Adresse für Onboard

Administrator von einem DHCP-Server. Das Kontrollkästchen „Standby“ wird nur angezeigt, wenn sich im Gehäuse ein Onboard Administrator Standby-Modul befindet.

- **Enable Dynamic DNS** (Dynamisches DNS aktivieren): Ermöglicht die Verwendung des gleichen Hostnamens für den Onboard Administrator über eine Zeitspanne hinweg, obwohl sich die dynamisch zugewiesene IP-Adresse ändern könnte. Der Hostname wird bei einem DNS-Server registriert. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Aufzeichnungen für IP-Adressen.

  Wenn „Dynamic DNS“ (Dynamisches DNS) auf Onboard Administrator deaktiviert wird, werden die Onboard Administrator-Aktualisierungen am DNS-Server gestoppt. Es ist jedoch zu beachten, dass bei einigen DHCP-Servern eine Regelung die direkte Aktualisierung von DNS-Servern ermöglicht. Um dynamische DNS-Aktualisierungen vollständig zu deaktivieren, müssen Sie „Dynamic DNS“ (Dynamisches DNS) sowohl auf dem Onboard Administrator als auch auf dem DHCP-Server deaktivieren.

- **Use static IP settings for each Active (or Standby) Onboard Administrator** (Statische IP-Einstellungen für jeden aktiven (oder Standby-) Onboard Administrator verwenden) – Dient zum manuellen Einrichten statischer IPEinstellungen für den Onboard Administrator. Das Kontrollkästchen „Standby“ wird nur angezeigt, wenn sich im Gehäuse ein Onboard Administrator Standby-Modul befindet.

⚠ **ACHTUNG:** Wenn DHCP für IPv4 aktiviert wird, gehen alle statischen IPv4-Einstellungen verloren.

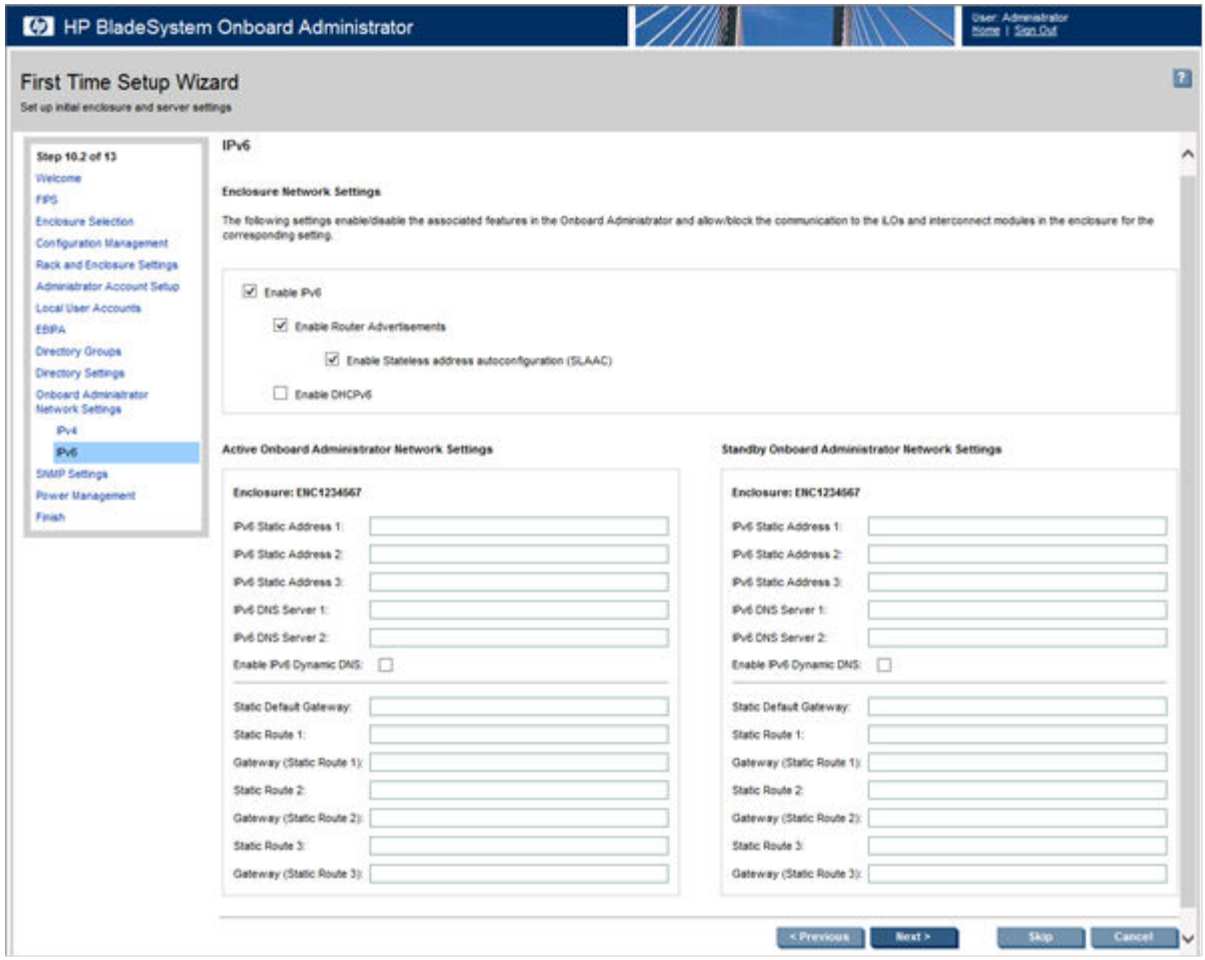
Feld	Möglicher Wert	Beschreibung
DNS Host Name (DNS-Hostname)	1 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Der DNS-Hostname des Onboard Administrator. Diese Einstellung gilt für IPv4- und IPv6-Umgebungen. Der DNS-Hostname kann entweder über DHCP oder über statische IP-Einstellungen zugewiesen werden. Eine Änderung des Onboard Administrator-DNS-Namens kann zu Unstimmigkeiten mit dem Hostnamen auf dem SSL-Zertifikat führen. Möglicherweise müssen die Zertifikatinformationen auf dem betroffenen Onboard Administrator über den Bildschirm „Certificate Administration“ (Zertifikatverwaltung) des aktiven Onboard Administrator-Moduls (Registerkarte „Certificate Administration Information“ (Zertifikatsverwaltungsinformationen) auf Seite 216) bzw. über den Bildschirm „Certificate Administration“ (Zertifikatverwaltung) des Standby-Onboard Administrator-Moduls (Registerkarte „Information“ (Informationen) auf dem Bildschirm „Standby Onboard Administrator Certificate Administration“ (Zertifikatverwaltung des Onboard Administrator-Standby-Moduls) auf Seite 232) aktualisiert werden.
IP Address (SLAAC-Adresse)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Statische IP-Adresse für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).
Subnet Mask (Subnetzmaske)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Subnetzmaske für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).
Gateway	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Gatewayadresse für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).

Feld	Möglicher Wert	Beschreibung
DNS Server 1 (DNS-Server 1)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IP-Adresse des primären IPv4 DNS-Servers.*
DNS Server 2 (DNS-Server 2)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IPv4-Adresse des sekundären IPv4 DNS-Servers.*

* Die Reihenfolge, in der Onboard Administrator DNS-Server verwendet, wird auf der Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) (Registerkarte „IPv4-Einstellungen“ auf Seite 126) beschrieben.

Um die neuen IPv4-Einstellungen zu speichern, klicken Sie auf **Next** (Weiter).

Bildschirm des Assistenten für die Erstkonfiguration (First Time Setup Wizard) für die IPv6-Netzwerkeinstellungen



IPv6-Netzwerkeinstellungen des Assistenten für die Erstkonfiguration (First Time Setup Wizard)

IPv6 unterstützt mehrere Adressen. Es können beliebige Kombinationen der Netzwerkeinstellungen aktiviert werden. Bei Aktivierung von IPv6, SLAAC und/oder DHCPv6 kann der Onboard Administrator von allen ausgewählten Quellen IP-Adressen beziehen. Er kann über automatisch zugewiesene IP-Adressen und vom Benutzer angegebene statische IP-Adressen verfügen. Die Einstellungen **Enable SLAAC** (SLAAC aktivieren), **Enable DHCPv6** (DHCPv6 aktivieren) und **Enable**

Router Advertisements (Routerankündigungen aktivieren) werden nur wirksam, wenn IPv6 aktiviert ist.

- **Enable IPv6** (IPv6 aktivieren): Aktiviert das IPv6-Protokoll für alle Onboard Administrator-, Verbindungs- und Server-iLO-Module im Gehäuse.
- **Enable Router Advertisements** (Routerankündigungen aktivieren): Ermöglicht IPv6-Routerankündigungen vom externen Verwaltungsnetzwerk im internen Gehäuseverwaltungsnetzwerk. Wenn Sie diese Einstellung deaktivieren, blockiert Onboard Administrator IPv6-Routerankündigungen, die vom externen Verwaltungsnetzwerk gesendet werden, wodurch sie am Eintritt in das interne Verwaltungsnetzwerk des Gehäuse gehindert werden.
- **Enable SLAAC** (SLAAC aktivieren): Aktiviert Benachrichtigungen über die zustandslose automatische Konfiguration von IPv6-Adressen an alle Onboard Administrator-, Verbindungs- und Server-iLO-Module im Gehäuse. Diese Funktion wirkt sich nur auf globale IPv6-Adressen aus.
- **Enable DHCPv6** (DHCPv6 aktivieren): Ermöglicht dem aktiven (und, sofern aktiviert, dem Standby-) Onboard Administrator, eine DHCPv6-IP-Adresse anzufordern. Ermöglicht DHCPv6-Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk.

ACHTUNG: Wenn Sie IPv6 in einer reinen IPv6-Umgebung deaktivieren, geht die Verbindung zur Onboard Administrator-GUI und allen SSH-Sitzungen verloren. Um die Verbindung wieder aufzubauen, müssen Sie die Erstkonfiguration des Gehäuses über das IPv4-Netzwerk, das Insight Display oder die serielle Schnittstelle der Onboard Administrator-Konsole vornehmen. Wenn Sie IPv6, SLAAC oder DHCPv6 deaktivieren, werden alle Verbindungen, die vom deaktivierten Protokoll abhängig sind, geschlossen. Angenommen, Sie sind mit dem Onboard Administrator über dessen DHCPv6-zugewiesene Adresse verbunden. Wenn die DHCPv6-Einstellung des Gehäuses deaktiviert wird, hat dies zur Folge, dass Ihre Sitzung geschlossen wird.

HINWEIS: Damit SLAAC-Adressen erfolgreich konfiguriert werden, müssen die Einstellungen **Enable SLAAC** (SLACC aktivieren) und **Enable Router Advertisements** (Routerankündigungen aktivieren) auf dem Gehäuse aktiviert sein. Darüber hinaus muss ein IPv6-Router auf dem Gehäuse-Verwaltungsnetzwerk konfiguriert werden, um die SLAAC-Adressen über Routerankündigungen bereitzustellen. iLOs müssen zum Anfordern von SLAAC-Adressen möglicherweise separat konfiguriert werden. Die Einstellungen **Enable SLAAC** (SLAAC aktivieren), **Enable Router Advertisements** (Routerankündigungen aktivieren) und **Enable IPv6** (IPv6 aktivieren) müssen aktiviert sein, um den erforderlichen Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk zu ermöglichen.

HINWEIS: Damit DHCPv6-Adressen erfolgreich konfiguriert werden, muss die Einstellung **Enable IPv6** (IPv6 aktivieren) aktiviert sein und auf dem Verwaltungsnetzwerk muss ein DHCPv6-Server konfiguriert sein. Alle iLOs und Verbindungsmodule müssen zum Anfordern einer DHCPv6-Adresse separat konfiguriert werden. Wenn sie zum Anfordern von DHCPv6-Adressen konfiguriert sind, müssen die Einstellungen **Enable IPv6** (IPv6 aktivieren) und **Enable DHCPv6** (DHCPv6 aktivieren) aktiviert sein, um den erforderlichen Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk zu ermöglichen.

HINWEIS: Nach dem Zurücksetzen auf die Werkseinstellungen sind die IPv6-Netzwerkeinstellungen für IPv6, SLAAC, DHCPv6 und Routerankündigungen des Gehäuses standardmäßig aktiviert.

Feld	Möglicher Wert	Beschreibung
IPv6 Static Address 1 (Statische IPv6 Adresse 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 1 des externen Onboard Administrator-NIC.
IPv6 Static Address 2 (Statische IPv6 Adresse 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 2 des externen Onboard Administrator-NIC.
IPv6 Static Address 3 (Statische IPv6 Adresse 3)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 3 des externen Onboard Administrator-NIC.
IPv6 DNS Server 1 (IPv6 DNS-Server 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt. Das Präfix ist optional.[1]	Die IPv6-Adresse des ersten statischen IPv6 DNS-Servers.[3]
IPv6 DNS Server 2 (IPv6 DNS-Server 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt. Das Präfix ist optional.[1]	Die IPv6-Adresse des zweiten statischen IPv6 DNS-Servers.[3]
Enable IPv6 Dynamic DNS (Dynamisches IPv6-DNS aktivieren)	Aktiviert (Kontrollkästchen ausgewählt) oder deaktiviert (Kontrollkästchen nicht ausgewählt).	Ermöglicht Ihnen, für den Onboard Administrator einen Hostnamen zu verwenden, der auch dann noch beibehalten wird, wenn sich die dynamisch zugewiesene IP-Adresse ändern sollte. Der Hostname ist bei einem DNS-Server registriert. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Datensätzen für IP-Adressen.[4] Wenn „Dynamic DNS“ (Dynamisches DNS) auf Onboard Administrator deaktiviert wird, werden die Onboard Administrator-Aktualisierungen am DNS-Server gestoppt. Es ist jedoch zu beachten, dass bei einigen DHCP-Servern eine Regelung die direkte Aktualisierung von DNS-Servern ermöglicht. Um dynamische DNS-Aktualisierungen vollständig zu deaktivieren, müssen Sie „Dynamic DNS“ (Dynamisches DNS) sowohl auf dem Onboard Administrator als auch auf dem DHCP-Server deaktivieren.
Static Default Gateway (Statisches Standard-Gateway)	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix	Die statische IPv6-Adresse des Standard-Gateways. Diese Einstellung ist in einer IPv6-Netzwerkumgebung, die vollständig statisch konfiguriert wurde, erforderlich. Onboard Administrator kann die IPv6-Gatewaykonfiguration direkt über diese Einstellung und über Routerankündigungen

Feld	Möglicher Wert	Beschreibung
	an. Es wird vorausgesetzt, dass das Gateway vom Onboard Administrator-Netzwerk aus erreichbar ist.[1]	von IPv6-Routern im Verwaltungsnetzwerk akzeptieren, sofern Routerankündigungen konfiguriert sind. Wenn die IPv6-Gatewaykonfiguration über Routerankündigungen bereitgestellt wird, wird die statische IPv6-Gateway-Einstellung durch die Gatewaykonfiguration der Routerankündigungen übersteuert. Das derzeit von dem Onboard Administrator verwendete IPv6-Gateway wird auf dem Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) (Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator auf Seite 212) des aktiven Onboard Administrator und auf dem Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des Standby-Onboard Administrator im Feld „Current Default Gateway“ (Aktuelles Standard-Gateway) angezeigt.
Static Route 1 (Statischer Verbindungsweg 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration).[5] Der statische Verbindungsweg definiert einen expliziten Pfad, den der Onboard Administrator verwendet, um über ein Gateway ein externes Netzwerk zu erreichen. In einer statischen Netzwerkkonfiguration ist es aufgrund des statischen Verbindungswegs nicht notwendig, einen Router zum Senden von Verbindungsweginformationen über Routerankündigungen zu konfigurieren. Wenn in einem Netzwerk mit aktiven Routerankündigungen das Standard-Gateway bereits konfiguriert ist, teilt der Router allen Knoten die verfügbaren statischen Verbindungswege mit. In diesem Fall ist eine manuelle Konfiguration der statischen Verbindungswege nicht erforderlich. Wenn Sie den statischen Verbindungsweg 1 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 1) angeben.
Gateway (Static Route 1) (Gateway (Statischer Verbindungsweg 1))	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen Netzwerk aus erreichbar sein.[1]	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 1 definierten Pfades. Sie müssen auch den statischen Verbindungsweg 1 angeben.
Static Route 2 (Statischer Verbindungsweg 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen zweiten statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration). Wenn Sie den statischen Verbindungsweg 2 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 2) angeben.
Gateway (Static Route 2) (Gateway (Statischer Verbindungsweg 2))	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 2 definierten Pfades. Sie müssen auch den statischen Verbindungsweg 2 angeben.

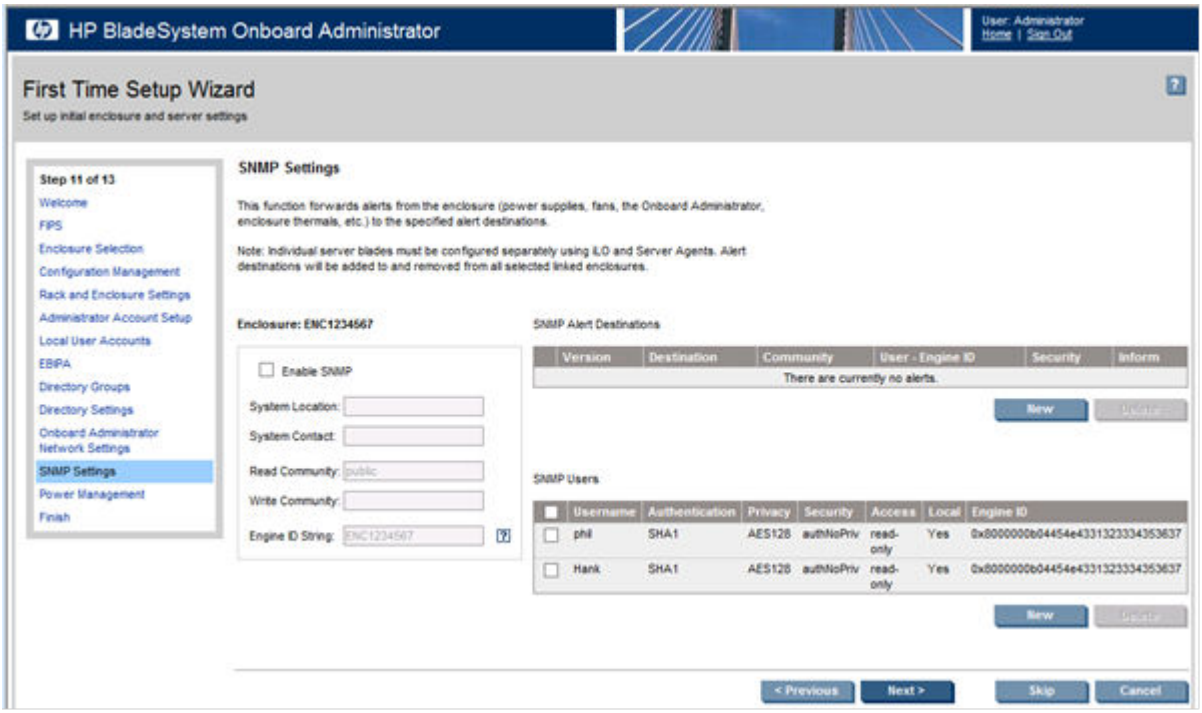
Feld	Möglicher Wert	Beschreibung
	Netzwerk aus erreichbar sein.[1]	
Static Route 3 (Statischer Verbindungsweg 3)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen dritten statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration). Wenn Sie den statischen Verbindungsweg 3 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 3) angeben.
Gateway (Static Route 3) (Gateway (Statischer Verbindungsweg 3))	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen Netzwerk aus erreichbar sein.[1]	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 3 definierten Pfades. Sie müssen auch den statischen Verbindungsweg 3 angeben.

[1] Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
[2] Der Onboard Administrator akzeptiert als statische IPv6-Adresse keine verbindungslokale Adresse.
[3] Die Reihenfolge, in der Onboard Administrator DNS-Server verwendet, wird auf der Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) (Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf Seite 129) beschrieben.
[4] Für „IPv6 Dynamic DNS“ (Dynamischer IPv6-DNS) muss auf dem Onboard Administrator ein gültiger DNS-Server (entweder IPv4 oder IPv6) konfiguriert sein.
[5] **Achtung**: Das Hinzufügen oder Entfernen eines statischen Verbindungsweges kann zum Verlust der Konnektivität von Clients führen, die auf Onboard Administrator zugreifen.

Um die IPv6-Einstellungen zu speichern, klicken Sie auf **Next** (Weiter).

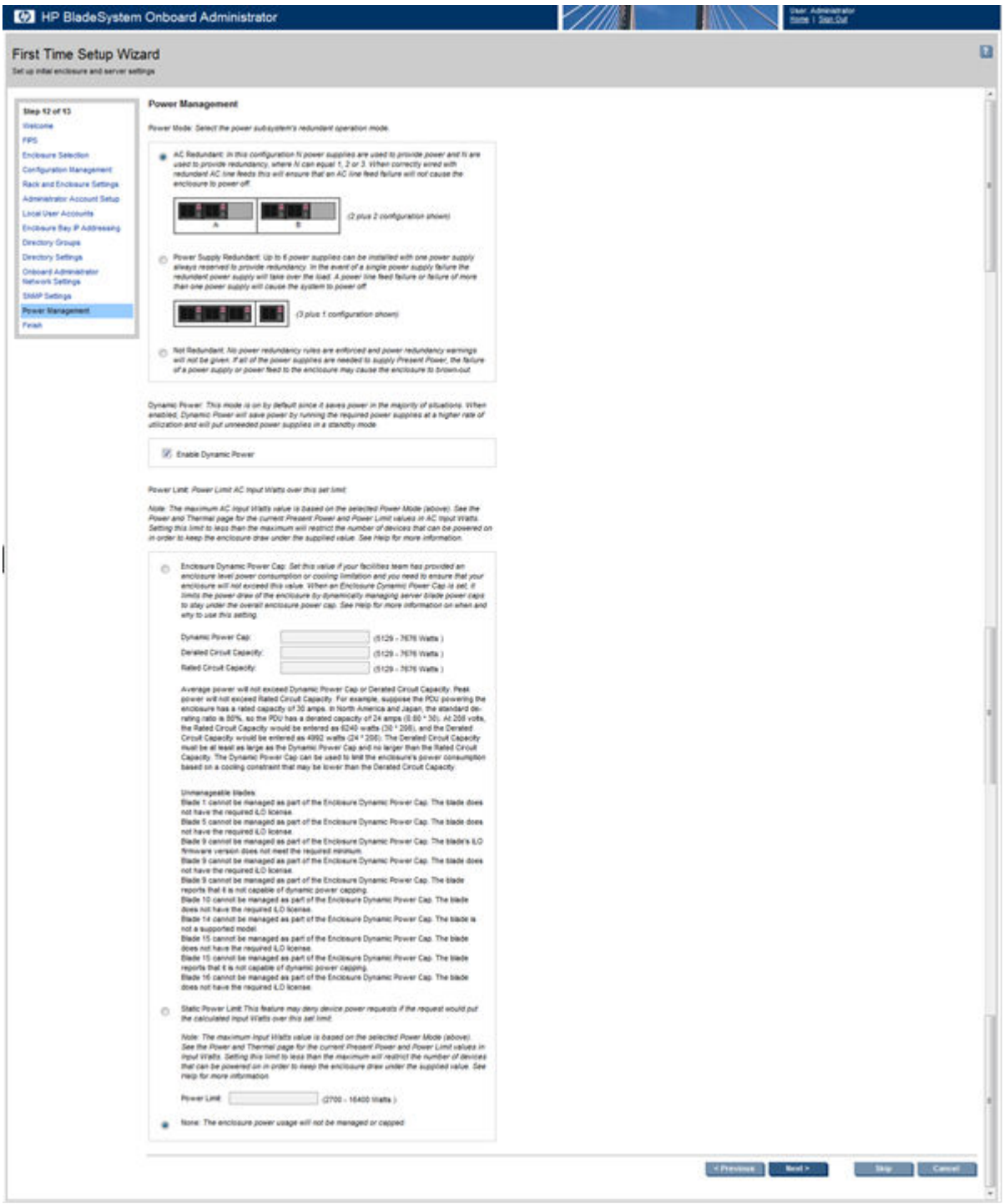
Bildschirm „Enclosure SNMP Settings“ (SNMP-Gehäuseeinstellungen)

Verwenden Sie den Bildschirm „Enclosure SNMP Settings“ (SNMP-Gehäuseeinstellungen), um die SNMP-Einstellungen für das aktive HP BladeSystem Onboard Administrator-Modul zu konfigurieren oder zu ändern.



Mögliche Werte sowie eine Beschreibung der einzelnen Felder finden Sie unter „SNMP-Einstellungen“ (SNMP-Einstellungen auf Seite 143).

Bildschirm „Power Management“ (Stromversorgungsverwaltung)



HINWEIS: Wenn als Redundanzmodus „Redundant“, „AC Redundant“ (Netzredundant) oder „Power Supply Redundant“ (Netzteilredundant) eingestellt ist und die Stromversorgungsredundanz verloren geht, müssen Sie entweder zusätzliche Netzteile hinzufügen oder die Einstellung für den Redundanzmodus in Onboard Administrator ändern, um den Status des Stromversorgungs-Subsystems wiederherzustellen. Korrektive Maßnahmen sind im Insight Display zu finden.

HINWEIS: Um den Stromredundanzmodus zu ändern, müssen Sie die dynamische Stromobergrenze des Gehäuses deaktivieren. Setzen Sie die dynamische Stromobergrenze des Gehäuses nach Ändern des Stromredundanzmodus auf die neuen Bereiche zurück.

Stromverwaltungsoptionen

Die Stromverwaltungssysteme der HP BladeSystem c3000- und c7000-Gehäuse ermöglichen Ihnen, Ihr Gehäuse gemäß Ihren Anforderungen zu konfigurieren. Auf dem Bildschirm „Onboard Administrator Power Management“ (Onboard Administrator-Stromversorgungsverwaltung) stehen unterschiedliche Stromverwaltungsoptionen zur Auswahl. Diese Stromverwaltungsoptionen werden in der folgenden Tabelle beschrieben.

Stromverwaltungsoption	Insight Display-Name	Beschreibung
Stromversorgungsmodus (Redundanzmodus)		
„Redundant“ oder „AC Redundant“ (Wechselstromredundant)	„Redundant“ oder „AC Redundant“ (Wechselstromredundant)	Der OA erkennt den Typ der vorhandenen Netzteile, passt das Verhalten des Stromversorgungsmodus automatisch entsprechend an und zeigt die zugehörige Modusbezeichnung an: • Wenn Gleichstromnetzteile vorhanden sind: Modus „Redundant“ • Wenn Wechselstromnetzteile vorhanden sind: Modus „AC Redundant“ (Wechselstromredundant) Wird auch als N+N-Redundanz oder Stromnetzredundanz bezeichnet. *N* Netzteile werden zur Stromversorgung und *N* Netzteile werden zur Sicherung der Redundanz verwendet (dabei kann *N* 1, 2 oder 3 sein). Es können bis zu drei Netzteile ausfallen, ohne dass das Gehäuse ausfällt. Bei korrekter Verdrahtung mit redundanten AC- und DC-Zuleitungen stellt diese Konfiguration auch sicher, dass das Gehäuse bei einem Ausfall einer AC- oder DC-Zuleitung nicht ausgeschaltet wird. Sollte der unwahrscheinliche Fall eintreten, dass mehr als ein Netzteil aufgrund von Ausfällen mehrerer Netzteile oder des Stromnetzes keinen Strom mehr liefern kann, dann wird das System möglicherweise ausgeschaltet. Das System wird ausgeschaltet, wenn der Strom, der von den noch funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt.
Power Supply Redundant (Netzteilredundant)	Power Supply (Netzteil)	Für alle Netzteile. Dieser Modus unterstützt zwei bis sechs Netzteile. Dies wird auch als N+1-Redundanz bezeichnet. Bei diesem Stromversorgungsmodus liefern *N* Netzteile den Strom und 1 Netzteil sichert die Redundanz (dabei kann *N* 1, 2, 3, 4 oder 5 sein). Wenn ein 3-Phasen-Stromeingangsmodul für das c7000 Gehäuse verwendet wird, empfiehlt HP 3 oder 6 aktive Netzteile (2+1 oder 5+1) für einen ordnungsgemäßen Phasenausgleich. Dieser Stromversorgungsmodus soll das System entwurfsgemäß bei Ausfall eines Netzteils schützen. Sollte der unwahrscheinliche Fall eintreten, dass mehr als ein Netzteil aufgrund von Ausfällen mehrerer Netzteile oder des Stromnetzes keinen Strom mehr liefern kann, dann wird das System möglicherweise ausgeschaltet. Das System wird ausgeschaltet, wenn der Strom, der von den noch funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt.
Not Redundant (Nicht redundant)	Keine	Für alle Netzteile. Dieser Modus unterstützt 1 bis 6 Netzteile. Bei diesem Stromversorgungsmodus liefern *N* Netzteile den Strom

Stromverwaltungsoption	Insight Display-Name	Beschreibung
		und kein Netzteil sichert die Redundanz (dabei kann *N* 1, 2, 3, 4, 5 oder 6 sein). Wenn ein 3-Phasen-Stromeingangsmodul für das c7000 Gehäuse verwendet wird, empfiehlt HP 3 oder 6 aktive Netzteile für einen ordnungsgemäßen Phasenausgleich. Es ist keine Stromversorgungsredundanz gegeben und es werden keine entsprechenden Warnungen ausgegeben. Wenn ein Netzteil aufgrund eines Ausfalls des Netzteils oder des Stromnetzes keinen Strom mehr liefern kann, wird das System möglicherweise ausgeschaltet. Es wird ausgeschaltet, wenn der Strom, der von den noch funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt. Dieser Stromversorgungsmodus wird für bereitgestellte Systeme in Produktionsumgebungen nicht empfohlen.
Modus „Dynamic Power“ (Dynamische Stromversorgung) (aktiviert oder deaktiviert)		
Dynamic Power (Dynamische Stromversorgung)	Dynamic Power (Dynamische Stromversorgung)	Bei Aktivierung versetzt die dynamische Stromversorgung ungenutzte Netzteile automatisch in den Standbymodus, um die Netzteileffizienz des Gehäuses zu erhöhen und dadurch den Stromverbrauch des Gehäuses bei niedrigem Strombedarf zu verringern. Bei erhöhtem Strombedarf wird die volle Leistung von Netzteilen im Standbymodus automatisch wiederhergestellt. Weitere Informationen über die dynamische Stromversorgung folgen dieser Tabelle.
Modus „Power Limit“ (Strombegrenzung)		
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Keine	Ermöglicht die Angabe eines Limits für den Stromverbrauch des Gehäuses. Die Leistungsaufnahme wird begrenzt, indem Stromobergrenzen von Server Blades dynamisch so verwaltet werden, dass die Gesamtstromobergrenze des Gehäuses nicht überschritten wird. Weitere Informationen finden Sie in der nachstehenden Tabelle zur Strombegrenzung.
Static Power Limit (Statische Strombegrenzung)	Power Limit (Strombegrenzung)	Eine optionale Einstellung zur Strombegrenzung. Jedes Mal, wenn Sie versuchen, eine Komponente einzuschalten, werden der gesamte Strombedarf der neuen Komponente sowie der bereits eingeschalteten Komponenten mit dieser statischen Strombegrenzung verglichen. Überschreitet der gesamte Strombedarf den Grenzwert, wird das Einschalten der neuen Komponente verhindert. Weitere Informationen über die statische Strombegrenzung und worin sie sich von der dynamischen Stromobergrenze des Gehäuses unterscheidet, finden Sie in der nachstehenden Tabelle zur Strombegrenzung.

HINWEIS: Unabhängig von dem aktivierten Redundanzmodus sind alle im Gehäuse vorhandenen betriebsfähigen Netzteile in der Regel aktiv und tragen zur Deckung des Strombedarfs des Gehäuses bei. Wenn der Modus der dynamischen Stromversorgung aktiviert ist, werden einige Netzteile möglicherweise automatisch in den Standbymodus geschaltet, um die Gesamteffizienz der Stromversorgung des Gehäuses zu steigern. Weitere Informationen finden Sie in der nachstehenden Beschreibung des Modus der dynamischen Stromversorgung.

Mit Onboard Administrator kann der eingestellte Stromversorgungsmodus (Redundanz) geändert werden, nachdem das Gehäuse und die Geräte eingeschaltet wurden. Wenn der Stromversorgungsmodus geändert wird, aktualisiert Onboard Administrator bei Bedarf den Redundanzstatus und meldet beeinträchtigte bzw. ausgefallene Redundanz, sofern zutreffend. Zum Beispiel: Der ursprüngliche Stromversorgungsmodus war beim Einschalten aller Blades „Power Supply Redundant“ (Netzteilredundant) (N+1) und wurde dann auf „AC Redundant“ (Wechselstromredundant) (N+N) geändert. In diesem Fall stellt sich dem Onboard Administrator eine reduzierte Stromkapazität dar. Solange genug Strom verfügbar ist, bleiben alle Blades in Betrieb. Unter bestimmten Umständen wird ein Blade, z. B. wenn er einen anderen Server Blade ersetzt, jedoch nicht eingeschaltet. Weitere Informationen finden Sie in der nachstehenden Tabelle und in den sich daran anschließenden Abschnitten.

Dynamic Power (Dynamische Stromversorgung): Die Standardeinstellung ist „Disabled“ (Deaktiviert). Die folgenden Optionen können ausgewählt werden:

- Enabled (Aktiviert): Einige Netzteile können automatisch in den Standby-Betrieb geschaltet werden, um die Gesamteffizienz des Stromversorgungs-Subsystems des Gehäuses zu steigern.
- Disabled (Deaktiviert): Alle Netzteile teilen die Last. Die Effizienz des Stromversorgungssubsystems ist je nach Last unterschiedlich.

HINWEIS: Die Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus) wird bei allen c3000-Netzteilen unterstützt. Sie wird bei allen c7000-Netzteilen außer solchen unterstützt, die mit niedriger Eingangsspannung (Nennwert 100-120 VAC) betrieben werden.

HINWEIS: Bei OA v4.01 und höher wurde der werksseitig eingestellte Standardwert, der mit der Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus) verknüpft ist, aktiviert. Die Betriebseffizienz der derzeit verfügbaren HP Gold (92%ige Effizienz) und HP Platinum (94%ige Effizienz) Gehäuse-Netzteile macht diese firmwarebasierte Stromverwaltungsstrategie überflüssig. Die Einstellung für „Dynamic Power“ (Dynamischer Stromsparmodus) wird nur für HP Gehäuse-Netzteile mit einem Effizienzwert von weniger als 92 % empfohlen. Bei der Aktualisierung auf OA v4.01 oder höher wird die aktuelle Einstellung für „Dynamic Power“ (Dynamischer Stromsparmodus) nach der Aktualisierung beibehalten. Weitere Informationen finden Sie im Kundenratschlag c03957955 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03957955).

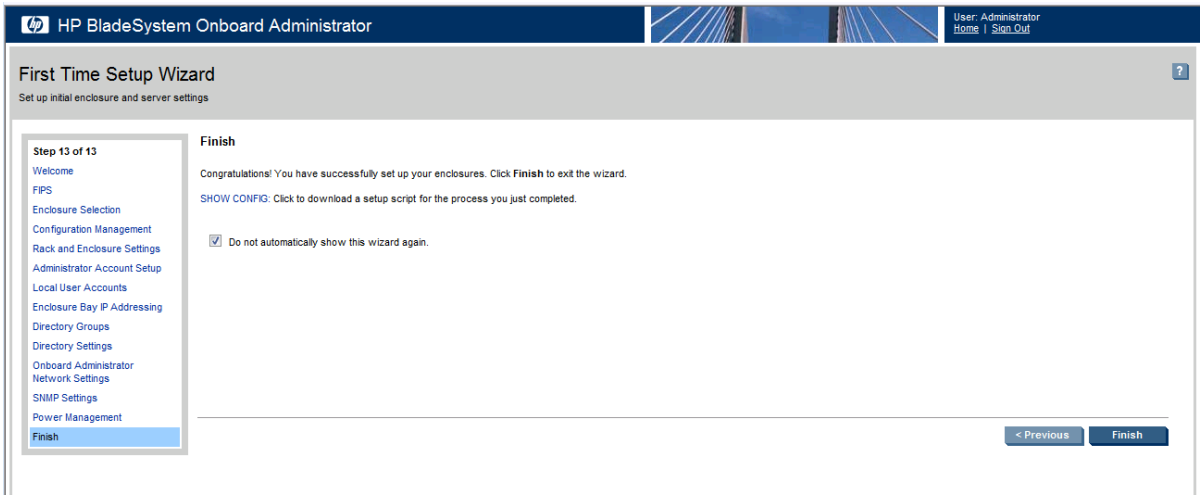
Power Limit (Strombegrenzung)

Legen Sie für ein leeres Gehäuse keinen Wert für „Static Power Limit“ (Statische Strombegrenzung) oder „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) fest.

Modus	Insight Display-Name	Beschreibung
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Keine	Eine optionale Funktion, mit der Sie eine Stromobergrenze für eine Gruppe von Servern in einem Gehäuse festlegen können. Wenn die Server ausgeführt werden, ändert sich der Strombedarf für jeden Server. Für jeden Server wird die Stromobergrenze automatisch angepasst, um den Server mit genug Strom zu versorgen, damit er seine Arbeitsauslastungsanforderungen erfüllen kann, während er gleichzeitig die dynamische Stromobergrenze des Gehäuses einhält. Es ist eine redundante Onboard Administrator-Platine erforderlich, um die Funktion „Dynamic Power Cap“ (Dynamische Stromobergrenze) einzurichten. Die Funktion wird mit drei Konfigurationsparametern aktiviert: • Dynamic Power Cap (Dynamische Stromobergrenze): Die durchschnittliche Stromversorgung überschreitet die dynamische Stromobergrenze insgesamt nicht.

Modus	Insight Display-Name	Beschreibung
		• Derated Circuit Capacity (Herabgesetzte Schaltkreis-Kapazität): Die durchschnittliche Stromleistung auf einem einzelnen Schaltkreis überschreitet nicht die herabgesetzte Schaltkreiskapazität. • Rated Circuit Capacity (Nennkapazität des Schaltkreises): Die Stromspitzenleistung auf einem einzelnen Schaltkreis überschreitet nicht die Nennkapazität des Schaltkreises. Wenn diese Parameter konfiguriert werden, muss der Wert für „Derated Circuit Capacity“ (Herabgesetzte Schaltkreiskapazität) mindestens so groß sein wie der Wert für „Dynamic Power Cap“ (Dynamische Stromobergrenze) und nicht größer als der Wert für „Rated Circuit Capacity“ (Nennkapazität des Schaltkreises). Mit der dynamischen Stromobergrenze wird der Stromverbrauch des Gehäuses infolge einer Kühlungsauflage eingeschränkt, die einen niedrigeren Wert als die herabgesetzte Schaltkreiskapazität vorschreibt. Mit der herabgesetzten Schaltkreiskapazität wird der durchschnittliche Stromverbrauch des Gehäuses auf einem Schaltkreis begrenzt. Mit der Nennkapazität des Schaltkreises wird der Spitzenstromverbrauch des Gehäuses auf einem Schaltkreis begrenzt. Wenn Sie die elektrische Last oder abgegebene Wärme eines Gehäuses begrenzen möchten, ist eine dynamische Stromobergrenze des Gehäuses (Enclosure Dynamic Power Cap) dafür besser geeignet als eine statische Strombegrenzung (Static Power Limit). Bei einer dynamischen Stromobergrenze können mehr Blades eingeschaltet werden als bei einer statischen Strombegrenzung. Eine komplette Liste der durch die Option „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) unterstützten BladeSystem Server Blades finden Sie auf der HP Website (http://www.hp.com/go/dpc).
Static Power Limit (Statische Strombegrenzung)	Power Limit (Strombegrenzung)	Eine optionale Einstellung zur Strombegrenzung. Jedes Mal, wenn Sie versuchen, eine Komponente einzuschalten, werden der gesamte Strombedarf der neuen Komponente sowie der bereits eingeschalteten Komponenten mit dieser statischen Strombegrenzung verglichen. Überschreitet der gesamte Strombedarf den Grenzwert, wird das Einschalten der neuen Komponente verhindert. Unter den folgenden Bedingungen ist eine statische Strombegrenzung besser geeignet: • Die Obergrenzen sollen nicht dynamisch für die Blades angepasst werden. • Sie ziehen es vor, einen Server Blade nicht einzuschalten, wenn ihm nicht die volle Stromversorgung zugewiesen werden kann (auch wenn er in der Regel weniger Strom verbraucht). • Mehr als 1/4 der Blades im Gehäuse erfüllen nicht die Hardware- oder Firmwareanforderungen für die dynamische Stromobergrenze des Gehäuses.
Keine	Keine	Der Stromverbrauch des Gehäuses wird nicht verwaltet oder begrenzt.

Finish (Fertig stellen)



So zeigen Sie eine aktuelle Konfiguration für das Gehäuse an:

1. Klicken Sie auf den Link **SHOW CONFIG** (Konfiguration anzeigen). Die Konfiguration wird in einem neuen Browserfenster geöffnet.
2. Um die Konfiguration als Textdatei zu speichern, wählen Sie eine der folgenden Optionen aus:
   - Wählen Sie bei Verwendung von Microsoft Internet Explorer die Option **Speichern unter** aus.
   - Wählen Sie bei Einsatz von Mozilla Firefox die Option **Seite speichern unter** aus.
   - Wählen Sie bei Verwendung von Google Chrome die Option **Save Link As** (Link speichern unter) aus.

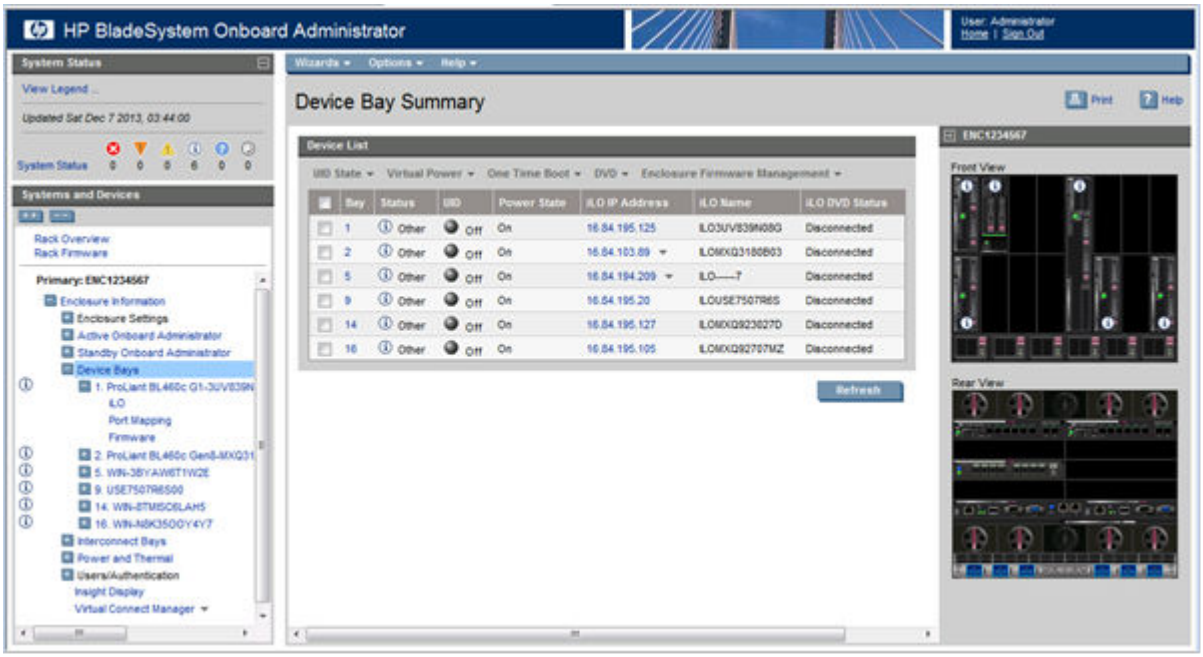
Aus Sicherheitsgründen enthält die abgerufene aktuelle Konfiguration keine Benutzerkennwörter. Sie können das Skript manuell bearbeiten und nach dem Benutzernamen in den ADD USER-Zeilen die Benutzerkennwörter einfügen. Außerdem enthält die abgerufene aktuelle Konfiguration keine der LCD-Einstellungen für „Lock Buttons“ (Tasten sperren), „Enable PIN Protection“ (PIN-Schutz aktivieren) und „PIN Code“ (PIN-Code). Diese Einstellungen können nicht aus dem Konfigurationsskript eingefügt werden.

Sie können das Kontrollkästchen **Do not automatically start this wizard again** (Diesen Assistenten nicht wieder automatisch starten) deaktivieren, damit der Assistent für die Erstkonfiguration (First Time Setup Wizard) bei der nächsten Anmeldung eines Benutzers bei Onboard Administrator erneut ausgeführt wird.

Klicken Sie auf **Finish** (Fertig stellen), um die Einstellungen zu speichern und den Assistenten für die Erstkonfiguration zu beenden. Der Bildschirm des Assistenten für die Erstkonfiguration wird geschlossen, und Sie kehren zum Standardhauptbildschirm von HP BladeSystem Onboard Administrator zurück.

6 Navigieren in Onboard Administrator

Navigationsübersicht

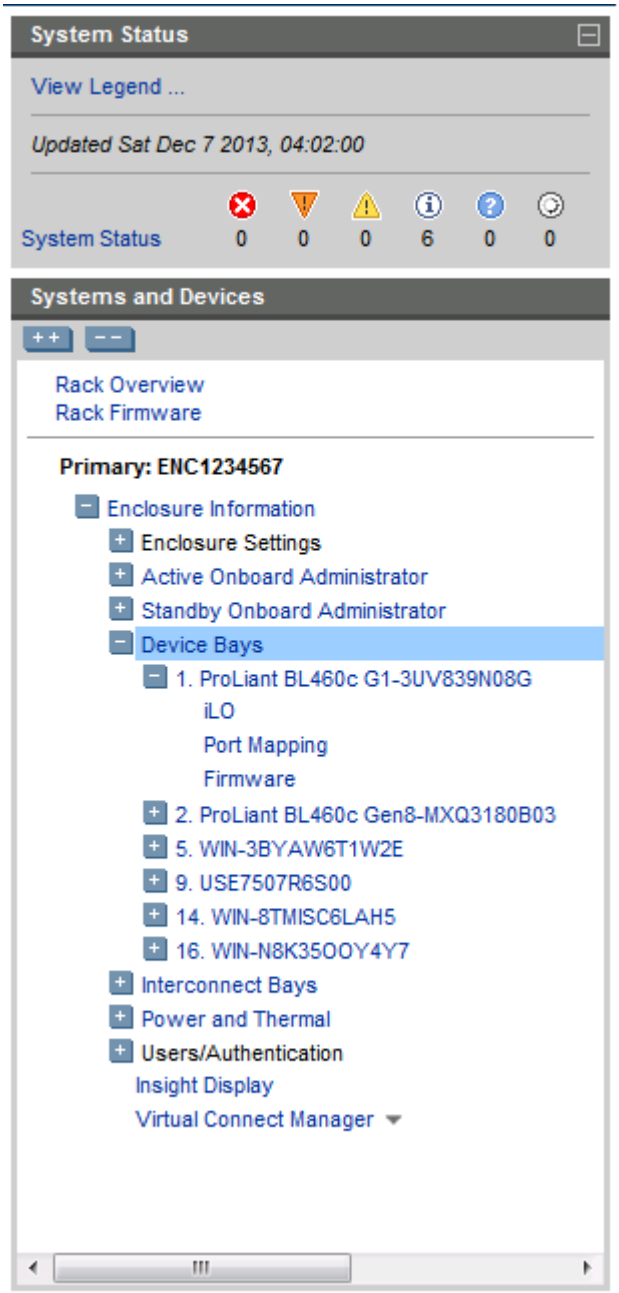


Das Hauptnavigationssystem des HP BladeSystem Onboard Administrator besteht aus einer Strukturansicht auf der linken Seite des Bildschirms, über die die Navigation durch die verschiedenen GUI-Bildschirme erleichtert wird. Sie bleibt beim Navigieren durch die Struktur sichtbar. In der Bildschirmmitte erscheinen Statusinformationen und Parameter, die Sie ändern können. Die rechte Seite des Bildschirms zeigt ein physisches Bild des Gehäuses. Sie können entweder mittels der Strukturansicht oder der grafischen Ansicht durch die durch die Gehäusegeräte und -funktionen navigieren.

Strukturansicht

Die Strukturansicht unterstützt Sie bei der Navigation durch die Komponenten und Funktionen für mehrere Gehäuse in einer hierarchischen Anordnung. Die Darstellung der Strukturansicht hängt von verschiedenen Faktoren ab, u. a. von den Benutzerberechtigungen, der Komponentenverfügbarkeit und dem Komponentenstatus. Wenn ein Benutzer als Bediener oder Benutzer konfiguriert ist, werden einige Optionen in der Strukturansicht unter Umständen nicht angezeigt.

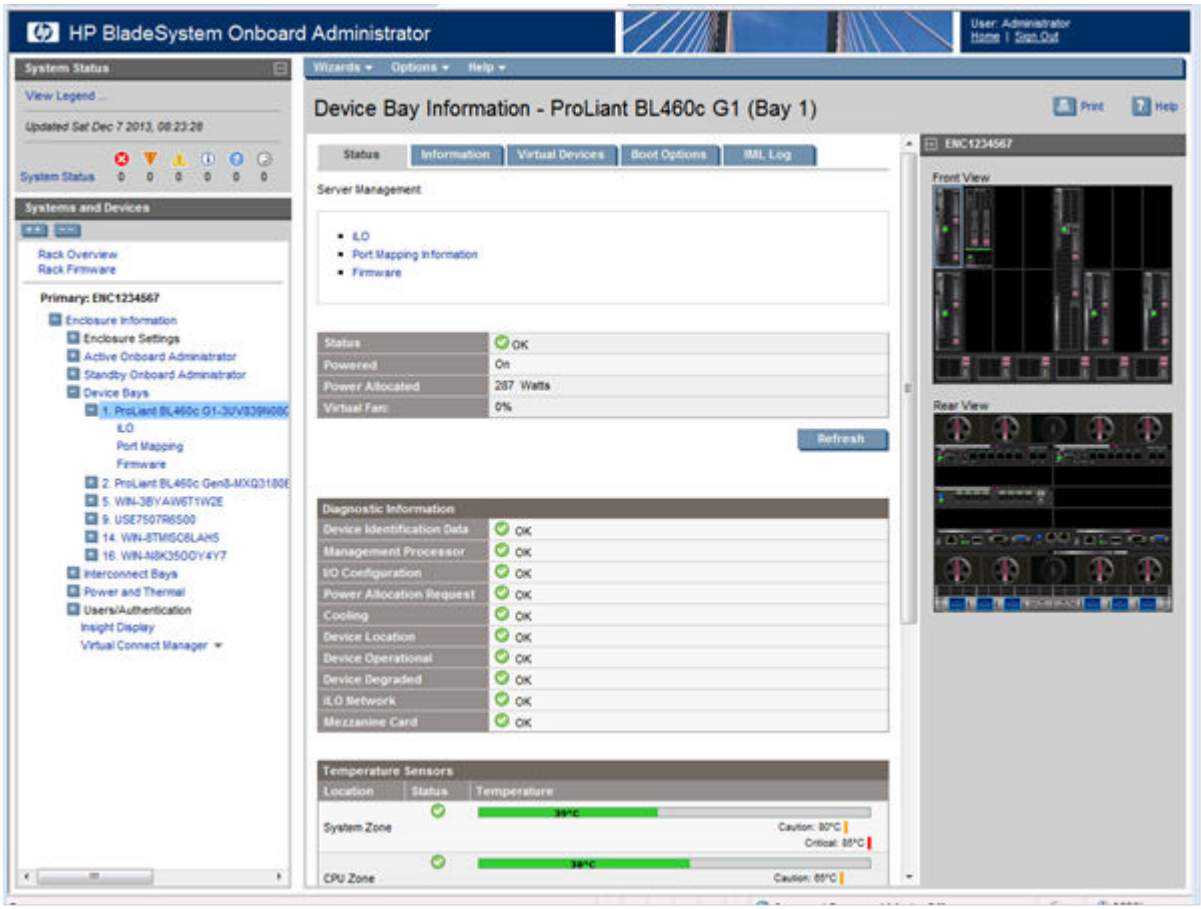
Die Strukturansichten für die c3000 und c7000 Gehäuse sind identisch.



Die Strukturansicht ermöglicht die Navigation anhand der auf den Hauptsystemen innerhalb des Gehäuses basierenden Kategorien. Wenn eine Kategorie durch Klicken auf das Zeichen + links neben der Kategorie erweitert wird, kann ein Symbol neben dem Kategorienamen auf einen beeinträchtigten Status des betroffenen Systems hinweisen. Bei einem Berichtsstatus für mehrere Komponenten kann das Statussymbol einen kumulativen Worst-Case-Status für alle Komponenten innerhalb derselben Kategorie angeben.

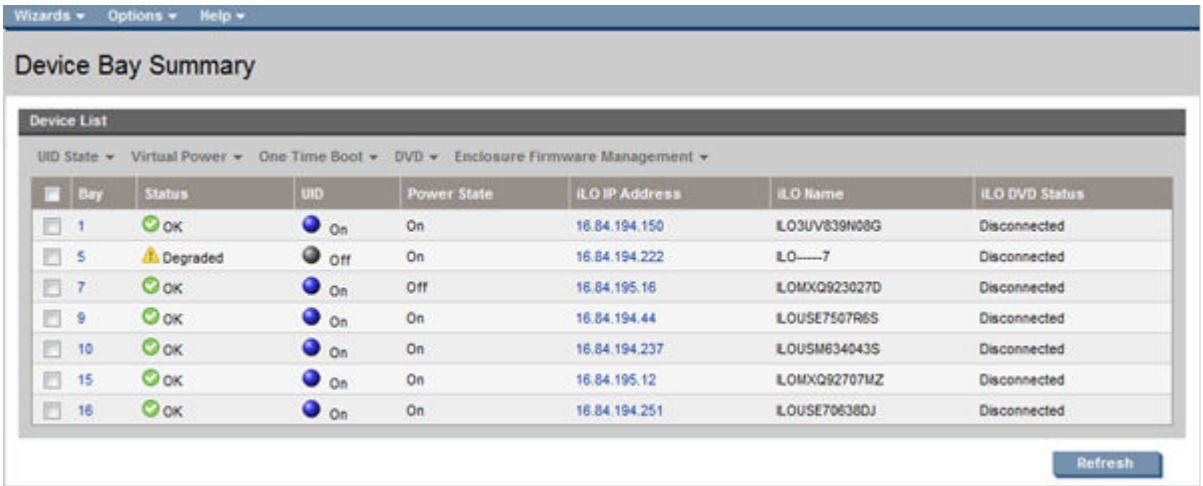
Einzelkomponentenseiten

Wenn Sie auf den Link für eine einzelne Komponente klicken, wird die Komponentendetailseite geöffnet, und die Komponente in der grafischen Ansicht im rechten Bereich der GUI wird ausgewählt. Die Einzelkomponentenseiten enthalten detaillierte Informationen über die ausgewählte Komponente sowie über alle anderen Funktionen für diese Komponente.



Kategoriezusammenfassungsseiten

Kategoriezusammenfassungsseiten enthalten zusammenfassende Informationen für die einzelnen Komponenten in der betreffenden Kategorie. Wenn Sie beispielsweise auf den Link **Device Bays** (Komponenteneinschübe) klicken, wird eine Einschubzusammenfassungsseite aufgerufen. Jedes übergeordnete Element in der Strukturansicht funktioniert auf diese Weise. Wenn Sie auf einen Kategoriezusammenfassungs-Link klicken, sind in der grafischen Navigationsansicht keine Komponenten ausgewählt.



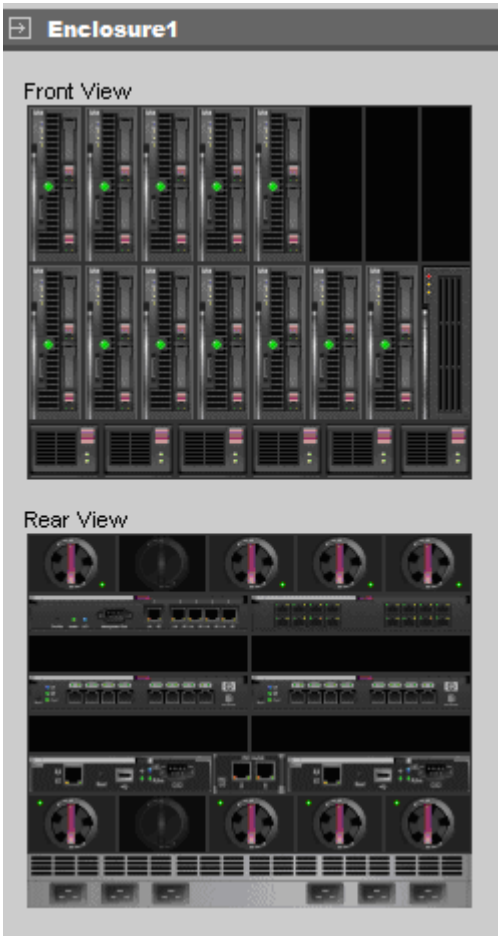
Systemformularseiten

Manche Komponenten, insbesondere HP Onboard Administrator, können Links zu verschiedenen Systemformularseiten aufweisen, die unter ihren Haupt-Links in der linken Strukturnavigationsansicht aufgeführt sind. Formularseiten enthalten Eingabetextfelder, Optionsschaltflächen und andere HTML-Eingabeelemente und werden zur Verwaltung der Einstellungen der Komponente verwendet, zu der sie gehören. Sie können zum Beispiel die Systemformularseite von HP Onboard Administrator verwenden, um die IP-Adresseneinstellungen zu ändern oder Firmware zu aktualisieren. Für diese Formulare sind unter dem übergeordneten Element von HP Onboard Administrator Links vorhanden. Wenn Sie auf einen Systemformular-Link klicken, wird die Komponente, zu der die Formularseite gehört, in der grafischen Ansicht ausgewählt. Klicken Sie beispielsweise auf den Link **Firmware Update** (Firmware-Aktualisierung) für das aktive HP Onboard Administrator-Modul, um die aktive HP Onboard Administrator-Komponente in der grafischen Ansicht auszuwählen. Links zu Systemformularen zeigen keine Statussymbole an.

Navigation in der grafischen Ansicht

Die zweite Komponente des HP BladeSystem Onboard Administrator-GUI-Navigationssystems ist eine grafische Darstellung des Gehäuses, die so genannte grafische Ansicht. Die grafische Ansicht umfasst zwei Komponenten: eine Vorderansicht und eine Rückansicht.

Die folgende Abbildung zeigt die grafische Darstellung eines typischen c7000-Gehäuses.



Die folgende Abbildung zeigt die grafische Darstellung eines typischen c3000-Gehäuses.

Alle Funktionen und Merkmale zur Navigation der grafischen Ansicht sind bei den c3000 und c7000 Gehäusen identisch, sofern nicht anderweitig vermerkt.

Auswählen einer Komponente

Klicken Sie zur Auswahl einer Komponente auf die grafische Darstellung der betreffenden Komponente in der grafischen Vorder- oder Rückansicht. Wenn Sie eine Komponente auswählen, ändert sich die Farbe des Rahmens, der die Komponente umgibt, von Grau in Hellblau, um anzugeben, dass es sich um die aktuell ausgewählte Komponente handelt. Mit der Auswahl einer Komponente in der grafischen Ansicht wird die entsprechende Komponente in der linken Strukturnavigationsansicht ausgewählt. Jedes Mal, wenn Sie in einem Bereich des Navigationssystems eine Komponente auswählen, gibt das übrige Navigationssystem diese Komponentenauswahl wieder, indem es entsprechend aktualisiert wird.

Statusberichte

Die grafische Ansicht gibt den Status jeder Komponente im Gehäuse wieder. Der Status der einzelnen Komponenten wird an der Komponente durch ein kleines Statussymbol angegeben. Für Komponenten, die einwandfrei funktionieren und den Status „OK“ besitzen, wird kein Statussymbol angezeigt. Alle anderen Statuscodes werden jedoch als Statussymbole am Gerät angezeigt.

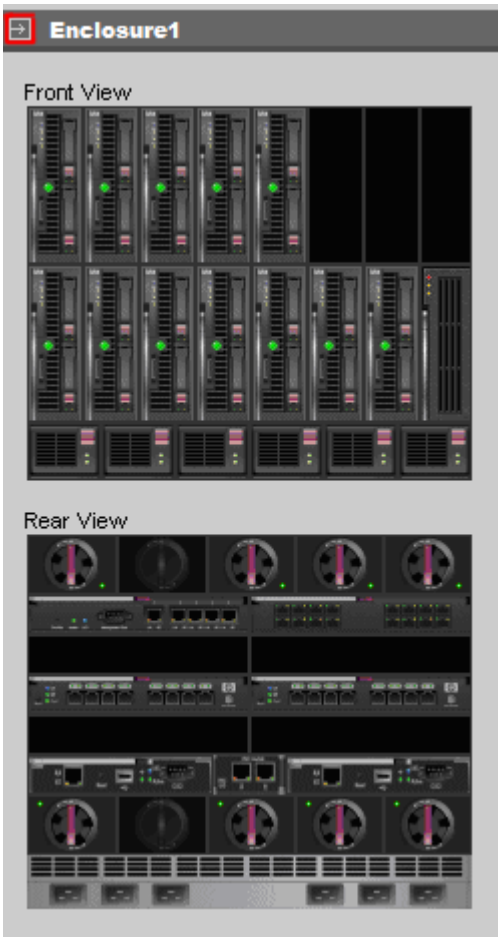
Die grafische Ansicht gibt keine Auskunft darüber, ob im Server Blade oder Speicher-Blade Festplattenlaufwerke enthalten sind.

Komponentensicherheit

Obwohl die grafische Vorder- und Rückansicht von den Benutzerberechtigungen abhängt, gelten für die grafische Ansicht andere Sicherheitsregeln als für die linke Strukturansicht. Wenn der Benutzer keine Zugriffsberechtigung für eine Komponente besitzt, wird ein leerer Einschub angezeigt, und zwar unabhängig davon, ob in diesem Einschub eine Komponente eingesetzt ist oder nicht, und in der Tabellenzelle des Einschubs wird ein Symbol in Form eines Vorhängeschlosses angezeigt, das angibt, dass der Einschub für den aktuellen Benutzer gesperrt ist.

Minimieren der grafischen Ansicht

Klicken Sie zur Minimierung der grafischen Ansicht in der Hauptanzeige auf das kleine Kästchen, das einen Pfeil enthält, direkt links neben dem Namen des Gehäuses in der grafischen Ansicht. Durch diese Option wird die grafische Ansicht minimiert, und es steht mehr Platz für den Hauptbereich der Anzeige zur Verfügung. Diese Funktion ist nützlich beim Anzeigen von Onboard Administrator auf einem kleinen Monitor oder auf Monitoren mit niedriger Auflösung.



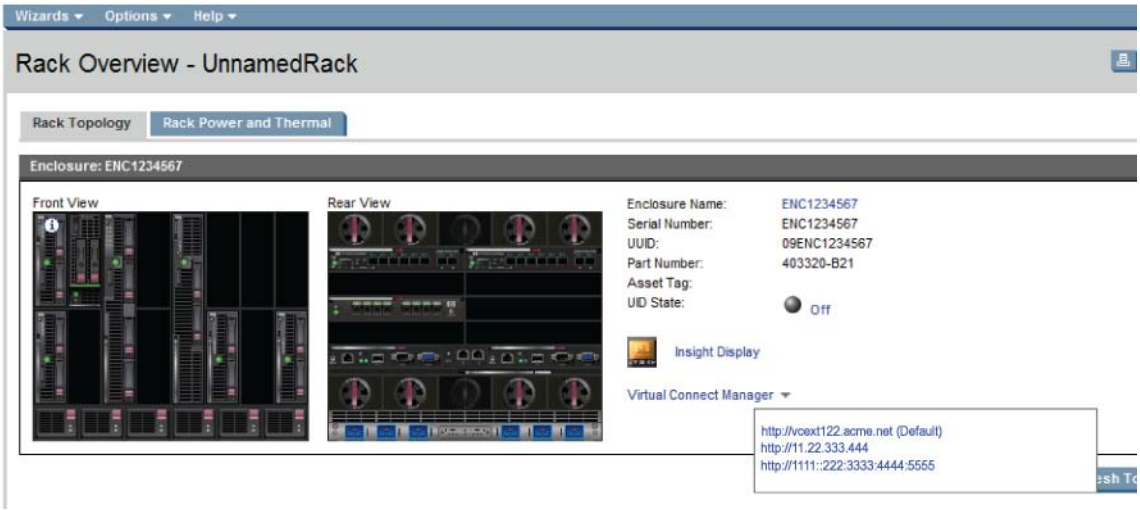
7 Ansicht des Racks

Bildschirm „Rack Overview“ (Rack-Übersicht)

Die Registerkarte „Rack Topology“ (Rack-Topologie) enthält eine grafische Darstellung des Gehäuses, die so genannte grafische Ansicht. Die grafische Ansicht umfasst eine Vorderansicht und eine Rückansicht. Wenn Sie den Mauszeiger auf einer Komponenten in der grafischen Ansicht platzieren, wird ein Fenster mit Informationen zur betreffenden Komponente geöffnet. Die grafische Ansicht zeigt den Status für jede Komponente im Gehäuse an und ermöglicht die Auswahl einzelner Komponenten zur Anzeige detaillierter Informationen.

Bei mehreren Gehäusen werden einige Gehäuse in der Rack-Übersicht möglicherweise abgeblendet dargestellt. Um den Inhalt und Informationen zu diesen Gehäusen anzuzeigen, geben Sie einen Benutzernamen und ein Kennwort in die Textfelder ein und klicken anschließend auf **Sign In** (Anmelden). Es wird eine grafische Ansicht des Gehäuses angezeigt. Die folgende Abbildung zeigt die Rack-Übersicht mit einem abgeblendeten Gehäuse.

Nach dem Anmelden wird der Gehäuseinhalt verfügbar, wie auf dem folgenden Beispielsbildschirm ersichtlich. Um eine Verbindung zu einem VCM herzustellen, klicken Sie auf den Abwärtspfeil neben „Virtual Connect Manager“. Ein Popup-Fenster zeigt die Internet-Adressen-Links an, über die eine Verbindung zu einem VCM hergestellt werden kann. Wenn FQDN-Link-Unterstützung aktiviert ist und bestimmte DNS-Konfigurationsvoraussetzungen erfüllt sind, ist eine FQDN-basierte VCM-Web-Adresse, wie veranschaulicht, die Standardauswahl. Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).



Rack-Informationen

Zeile	Beschreibung
Enclosure Name (Gehäusename)	Der vom Benutzer konfigurierte Name des Gehäuses im Rack.
Enclosure Rack U Position (Rack-U-Position des Gehäuses)	Die Position des Gehäuses im Rack.
Serial Number (Seriennummer)	Die eindeutige Seriennummer für das Gehäuse.
UUID	Der Universally Unique Identifier, der dem Gehäuse zugewiesen wurde.
Part Number (Artikelnummer)	Die Teilenummer des Gehäuses, die für ein neues Gehäuse oder ein Ersatzgehäuse verwendet wird.
Asset Tag (Systemkennung)	Die Systemkennung wird zur Bestandskontrolle verwendet.
UID State (UID-Status)	„On“ oder „Off“, abhängig davon, ob die UID ein- oder ausgeschaltet ist.

Rackpositions-Informationen

Zeile	Beschreibung
Rack Name (Rack-Name)	Der Name des Racks.
Rack Product Description (Rack-Produkt-Beschreibung)	Der allgemeine beschreibende Name des Racks.
Rack Part Number (Rack-Teilenummer)	Die Teilenummer für die Bestellung eines Ersatz-Racks.
Rack Identifier (Rack-Kennung)	Eine eindeutige Zeichenfolge, anhand der das Rack identifiziert wird.
Rack U Height (Rack-U-Höhe)	Die U-Höhe des Racks.

Verwenden der Location Discovery Services (Positionsermittlungsdienste)

„Location Discovery Services“ (Positionsermittlungsdienste) ist eine Komponente von HP Discovery Services. Location Discovery Services meldet HP SIM und Insight Control automatisch Serverpositionen, wodurch Server-Administratoren diese manuelle Aufgabe erspart bleibt.

Administratoren können die Positionsinformationen und Systemdaten mit HP Asset Manager verwenden, um genauere und vollständigere Bestandsdaten zu erhalten.

Location Discovery Services ist eine Rack-U-Positionsermittlungslösung für die Rack-Modelle G3 und höher. Die Komponente ermöglicht es HP iLO, BL Onboard Administrator und SL Chassis Firmware, Rack-ID und U-Position des Servers im Rack zu melden und anzuzeigen. Unterstützte Racks werden mit eindeutigen U- (Baueinheits-) Werten in 7U- und/oder 8U-Modulen programmiert und mit Tag-Versionsnummer, Rack-Kennung, Teilenummer, Produktnamen, Rack-Höhe und U-Position installiert. Location Discovery Services unterstützt 14U-, 22U-, 36U-, 42U- und 47U-Racks.

Das Rack-Gerät liest das U-Positions-Tag des Racks jedes Mal, wenn iLO mit Wechselstrom versorgt oder iLO zurückgesetzt wird. Der U-Positionswert bezeichnet die vom Gerät gelesene U-Position. Der Kontaktpositions-Versatz ist ein fester Wert pro Modell, der die Position des Kontakts relativ zur unteren U-Position des Geräts angibt. Er ist normalerweise 0, kann aber auch ein positiver Wert sein, wenn der Kontakt nicht in der unteren U-Position des Geräts platziert werden kann. Die vom Gerät belegte unterste U-Position wird berechnet, indem der U-Versatz von der U-Position subtrahiert wird.

Sie können die ermittelten Daten auf bestimmten Onboard Administrator-Bildschirmen, wie z. B. in der Tabelle „Rack Information“ (Rack-Informationen) auf der Registerkarte „Enclosure Information“ (Gehäuseinformationen) anzeigen. Zudem zeigen mehrere Onboard Administrator-CLI-Befehle die ermittelten Daten an, wie z. B. die Befehle `SHOW ENCLOSURE INFO` und `SHOW TOPOLOGY INFO`. Weitere Informationen zu diesen Befehlen finden Sie im *HP BladeSystem Onboard Administrator-Befehlszeilenschnittstelle Benutzerhandbuch*.

Rack Information	
Enclosure Rack U Position	21
Rack Product Description	HP 42U Intelligent Series Rack
Rack Part Number	BW946A
Rack Identifier	CN82190004
Rack U Height	42

Topologie-Modi

Onboard Administrator unterstützt drei Topologie-Modi, die durch die auf dem Anmeldebildschirm vor der Anmeldung getroffene Auswahl festgelegt werden. Folgende drei Topologie-Modi sind verfügbar:

- Modus „Local“ (Lokal) – Wird verwendet, um ein einzelnes Gehäuse zu verwalten, wenn mehrere Gehäuse ausgewählt werden können. Onboard Administrator ignoriert in diesem Modus alle Topologie-Änderungen. Dieser Modus ist nützlich, wenn die Topologie durch Hinzufügen weiterer miteinander verbundener Gehäuse nicht geändert werden soll.
- Modus „Linked“ (Verbunden) – Dient zur Verwaltung eines einzelnen Gehäuses, wenn keine anderen Gehäuse angeschlossen sind. Sie können den Modus „Linked“ (Verbunden) verwenden, um den Zusatz neuer Gehäuse zu ermöglichen, während diese zur Verkettung hinzugefügt werden. Solange keine neuen Gehäuse angeschlossen werden, scheint es so, als ob sich Onboard Administrator im Modus „Local“ (Lokal) befände. Alle Topologie-Änderungen, die auftreten, während der Benutzer angemeldet ist, werden von Onboard Administrator angezeigt. Dieser Modus bietet eine uneingeschränkte Ansicht der an der Verkettung angeschlossenen Gehäuse.
- Modus „Fixed“ (Fest) – Dient zur Verwaltung von mehr als einem, jedoch nicht allen Gehäusen. Nur Topologie-Änderungen, die sich auf die aktuelle Topologie auswirken, werden von Onboard

Administrator angezeigt. Dieser Modus ist zur Überwachung eines Teilsatzes aller an der Verkettung angeschlossenen Gehäuse nützlich.

Wenn als aktiver Modus ein einzelnes Gehäuse festgelegt wird und ein oder mehrere zusätzliche Gehäuse angeschlossen werden, müssen Sie sich abmelden und danach wieder anmelden, ohne ein verbundenes Gehäuse auszuwählen, wenn die zusätzlichen Gehäuse nicht in der Gehäusetopologie sichtbar sein sollen.

Registerkarte „Rack Topology“ (Rack-Topologie)

Die Registerkarte „Rack Topology“ (Rack-Topologie) enthält eine grafische Darstellung des Gehäuses, die so genannte grafische Ansicht. Die grafische Ansicht umfasst eine Vorderansicht und eine Rückansicht. Wenn Sie den Mauszeiger auf einer Komponenten in der grafischen Ansicht platzieren, wird ein Fenster mit Informationen zur betreffenden Komponente geöffnet. Die grafische Ansicht zeigt den Status für jede Komponente im Gehäuse an und ermöglicht die Auswahl einzelner Komponenten zur Anzeige detaillierter Informationen.

Auswählen einer Komponente

Klicken Sie zur Auswahl einer Komponente auf die grafische Darstellung der betreffenden Komponente in der grafischen Vorder- oder Rückansicht. Wenn Sie eine Komponente auswählen, ändert sich die Farbe des Rahmens, der die Komponente umgibt, von Grau in Hellblau, um anzugeben, dass es sich um die aktuell ausgewählte Komponente handelt. Mit der Auswahl einer Komponente in der grafischen Ansicht wird die entsprechende Komponente in der linken Strukturnavigationsansicht ausgewählt. Wenn Sie in einem Bereich des Navigationssystems eine Komponente auswählen, gibt das übrige Navigationssystem diese Komponentenauswahl wieder, indem es entsprechend aktualisiert wird.

Statusberichte

Die grafische Ansicht gibt den Status jeder Komponente im Gehäuse wieder. Der Status der einzelnen Komponenten wird an der Komponente durch ein kleines Statussymbol angegeben. Für Komponenten, die einwandfrei funktionieren und den Status „OK“ besitzen, wird kein Statussymbol angezeigt. Alle anderen Statuscodes werden jedoch als Statussymbole am Gerät angezeigt.

Die grafische Ansicht gibt keine Auskunft darüber, ob im Server Blade oder Speicher-Blade Festplattenlaufwerke enthalten sind.

Komponentensicherheit

Obwohl die grafische Vorder- und Rückansicht von den Benutzerberechtigungen abhängt, gelten für die grafische Ansicht andere Sicherheitsregeln als für die linke Strukturansicht. Wenn der Benutzer keine Zugriffsberechtigung für eine Komponente besitzt, wird ein leerer Einschub angezeigt, und zwar unabhängig davon, ob in diesem Einschub eine Komponente eingesetzt ist oder nicht, und in der Tabellenzelle des Einschubs wird ein Symbol in Form eines Vorhängeschlosses angezeigt, das angibt, dass der Einschub für den aktuellen Benutzer gesperrt ist.

Der Benutzer kann keinen gesperrten Einschub auswählen. Wenn der Benutzer den Mauszeiger auf dem gesperrten Einschub platziert, wird eine Meldung angezeigt, die besagt, dass der Benutzer keine Zugriffsberechtigung für die Komponente in diesem Einschub besitzt.

Rack-Informationen

Zeile	Beschreibung
Enclosure Name (Gehäusename)	Der vom Benutzer konfigurierte Name des Gehäuses im Rack.
Enclosure Rack U Position (Rack-U-Position des Gehäuses)	Die Position des Gehäuses im Rack.

Zeile	Beschreibung
Serial Number (Seriennummer)	Die eindeutige Seriennummer für das Gehäuse.
UUID	Der Universally Unique Identifier, der dem Gehäuse zugewiesen wurde.
Part Number (Artikelnummer)	Die Teilenummer des Gehäuses, die für ein neues Gehäuse oder ein Ersatzgehäuse verwendet wird.
Asset Tag (Systemkennung)	Die Systemkennung wird zur Bestandskontrolle verwendet.
UID State (UID-Status)	„On“ oder „Off“, abhängig davon, ob die UID ein- oder ausgeschaltet ist.

Um die Rack-Topologie zu aktualisieren, klicken Sie auf **Refresh Topology** (Topologie aktualisieren). Wenn Sie „Refresh Topology“ (Topologie aktualisieren) auswählen, wechselt der Bildschirms „Rack Topology“ (Rack-Topologie) in den Modus „Linked“ („Verbunden“), und alle verbundenen Gehäuse werden angezeigt.

Einige Racktopologie-Informationen werden über Positionsermittlungsdienste (Location Discovery Services) bereitgestellt. Weitere Informationen zur Verwendung von Positionsermittlungsdiensten (Location Discovery Services) finden Sie unter „Bildschirm ‚Rack Overview‘ (Rack-Übersicht)“ (Bildschirm „Rack Overview“ (Rack-Übersicht) auf Seite 100).

Linked enclosures (Verbundene Gehäuse)

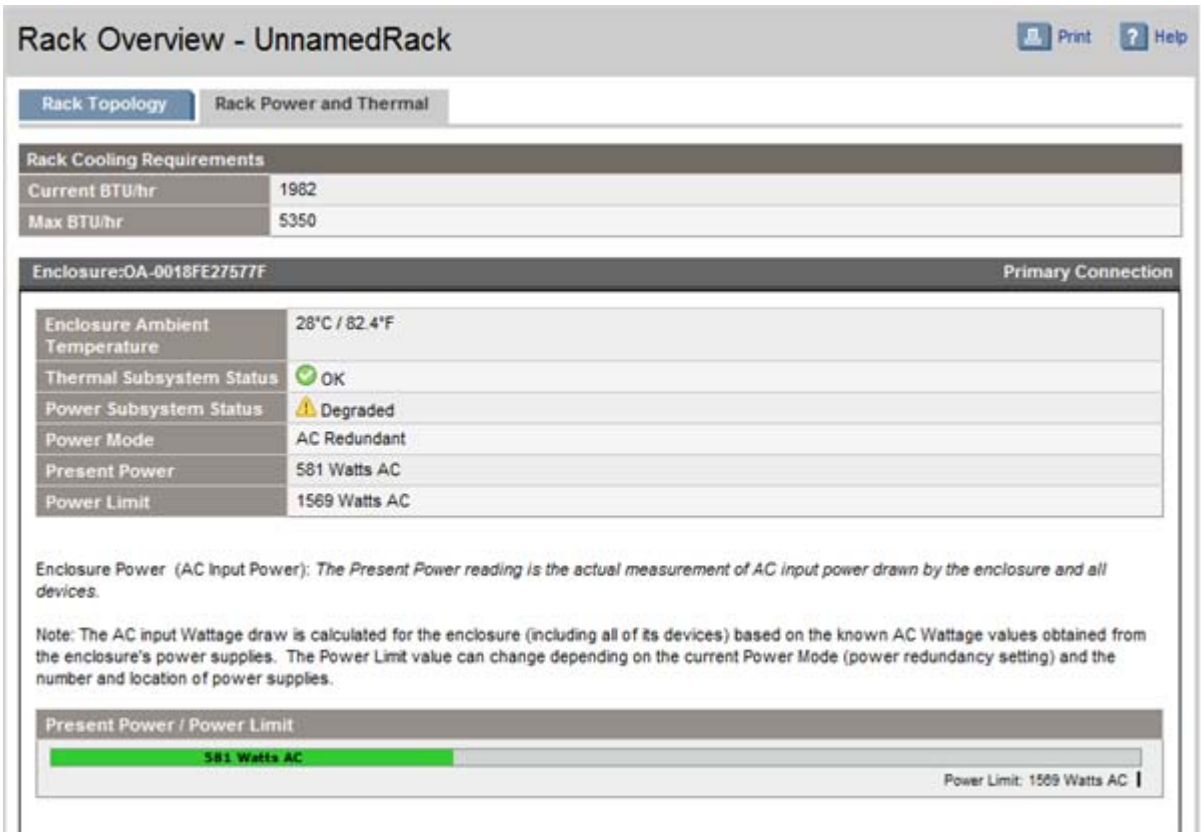
Auf der Registerkarte „Rack Topology“ (Rack-Topologie) werden alle verbundenen Gehäuse angezeigt, die sich in einem der folgenden Statuszustände befinden:

- Linked—Not Signed In (Verbunden – nicht angemeldet): Geben Sie einen Benutzernamen und ein Kennwort in die Textfelder ein, und klicken Sie auf **Sign In** (Anmelden). Es wird eine grafische Ansicht des Gehäuses angezeigt.
- „Linked-Not Signed In“ (Verbunden – Nicht angemeldet): Mit Kartenlesersymbol. Dieser Zustand gibt an, dass für das verbundene Gehäuse die 2-Faktor-Authentifizierung aktiviert ist, es aber nicht authentifiziert wurde. Dieser Zustand tritt unter zwei Bedingungen auf:
  - Wenn die Konfiguration nicht unterstützt wird. Für das primäre Gehäuse muss die 2-Faktor-Authentifizierung aktiviert sein und für das primäre und das verbundene Gehäuse müssen die gleichen Anmeldeinformationen gelten, damit das verbundene Gehäuse mit der 2-Faktor-Authentifizierung authentifiziert wird.
  - Wenn Sie bei einem Gehäuse mit aktivierter 2-Faktor-Authentifizierung, das bereits authentifiziert ist, auf den Link „Sign Out“ (Abmelden) klicken, wird dieser Zustand angezeigt. Um dieses Gehäuse erneut zu authentifizieren, müssen Sie die GUI aktualisieren und das primäre Gehäuse authentifizieren.
- „Linked—Signed In“ (Verbunden – angemeldet) mit der Schaltfläche „Load Enclosure Information“ (Gehäuseinformationen laden). Klicken Sie auf **Load Enclosure Information** (Gehäuseinformationen laden), um die grafische Ansicht des Gehäuses anzuzeigen.
- „Linked—Signed In“ (Verbunden – angemeldet): Mit einer grafischen Ansicht des angezeigten Gehäuses.

Klicken Sie auf **Sign Out** (Abmelden) rechts neben der Namensleiste des verbundenen Gehäuses, um sich von dem verbundenen Gehäuse abzumelden.

Registerkarte „Power and Thermal“ (Stromversorgung und Wärmewerte)

Die Registerkarte „Power and Thermal“ (Stromversorgung und Wärmewerte) zeigt Informationen über die Temperatur im Innern des Gehäuses sowie den Status des thermischen Subsystems und des Stromversorgungs-Subsystems an. Anhand einer grafischen Ansicht der aktuellen Stromversorgung und Strombegrenzung lässt sich der Stromversorgungsstatus bestimmen.


Rack Overview - UnnamedRack
Print
Help
Rack Topology
Rack Power and Thermal
Rack Cooling Requirements
Current BTU/hr
1982
Max BTU/hr
5350
Enclosure:OA-0018FE27577F
Primary Connection
Enclosure Ambient Temperature
28°C / 82.4°F
Thermal Subsystem Status
OK
Power Subsystem Status
Degraded
Power Mode
AC Redundant
Present Power
581 Watts AC
Power Limit
1569 Watts AC
Enclosure Power (AC Input Power): The Present Power reading is the actual measurement of AC input power drawn by the enclosure and all devices.
Note: The AC input Wattage draw is calculated for the enclosure (including all of its devices) based on the known AC Wattage values obtained from the enclosure's power supplies. The Power Limit value can change depending on the current Power Mode (power redundancy setting) and the number and location of power supplies.
Present Power / Power Limit
581 Watts AC
Power Limit: 1569 Watts AC

Rack-Kühlungsanforderungen

Zeile	Beschreibung
Current BTU/hr (Aktueller Wert BTU/Stunde)	Die Gesamtwärme, die von den miteinander verbundenen Gehäusen erzeugt wird, gemessen in BTU pro Stunde.
Max BTU/hr (Max. Wert BTU/Stunde)	Die maximale Wärme, die von den miteinander verbundenen Gehäusen unter Last erzeugt werden kann, gemessen in BTU pro Stunde.

Thermischer Status und Stromversorgungsstatus des Gehäuses

Zeile	Beschreibung
Enclosure Ambient Temperature (Gehäuseumgebungstemperatur)	Dieses Feld zeigt die höchste, von den installierten Blade-Komponenten gemeldete Umgebungstemperatur an. Sind keine Blade-Komponenten installiert, zeigt dieses Feld die Temperatur des Onboard Administrator-Moduls als eine Annäherung an die Umgebungstemperatur an.
Thermal Subsystem Status (Status des thermischen Subsystems)	Der allgemeine Wärmestatus des Gehäuses. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).

Zeile	Beschreibung
Power Subsystem Status (Status des Stromversorgungs-Subsystems)	Der allgemeine Stromversorgungsstatus des Gehäuses Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Power Mode (Stromversorgungsmodus)	Eine Benutzereinstellung zur Konfiguration der Gleichstromkapazität des Gehäuses und der Redundanz der Stromzufuhr des Gehäuses. Mögliche Werte werden unter „Power-Management“ aufgeführt.
Present Power (Aktueller Verbrauch)	Die Menge des von allen Komponenten im Gehäuse verbrauchten Stroms in Watt.
Power Limit (Strombegrenzung)	Der für den Verbrauch des Gehäuses maximal verfügbare Strom, gemessen in Watt.
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Eine für eine Gruppe von Servern im Gehäuse festgelegte Stromobergrenze. Wenn die Server ausgeführt werden, ändert sich der Strombedarf für jeden Server. Für jeden Server wird eine Stromobergrenze festgelegt, um den Server mit genug Strom zu versorgen, damit er seine Arbeitsauslastungsanforderungen erfüllen kann, während er gleichzeitig die dynamische Stromobergrenze des Gehäuses einhält. Durch kontinuierliche Überwachung des Strombedarfs und automatische Regulierung der Server-Stromobergrenzen wird sichergestellt, dass die Leistung nur minimal beeinträchtigt wird. Angaben zur Funktion „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) werden nur angezeigt, sofern eine Obergrenze definiert wurde.

HINWEIS: Wenn als Redundanzmodus „AC Redundant“ (Netzredundant) oder „Power Supply Redundant“ (Netzteilredundant) eingestellt ist und die Stromversorgungsredundanz verloren geht, müssen Sie entweder zusätzliche Netzteile hinzufügen oder die Einstellung für den Redundanzmodus in Onboard Administrator ändern, um den Status des Stromversorgungs-Subsystems wiederherzustellen. Korrektive Maßnahmen sind im Insight Display zu finden.

Present Power/Enclosure Dynamic Power Cap/Power Limit (Aktueller Verbrauch/Dynamische Stromobergrenze des Gehäuses/Strombegrenzung)

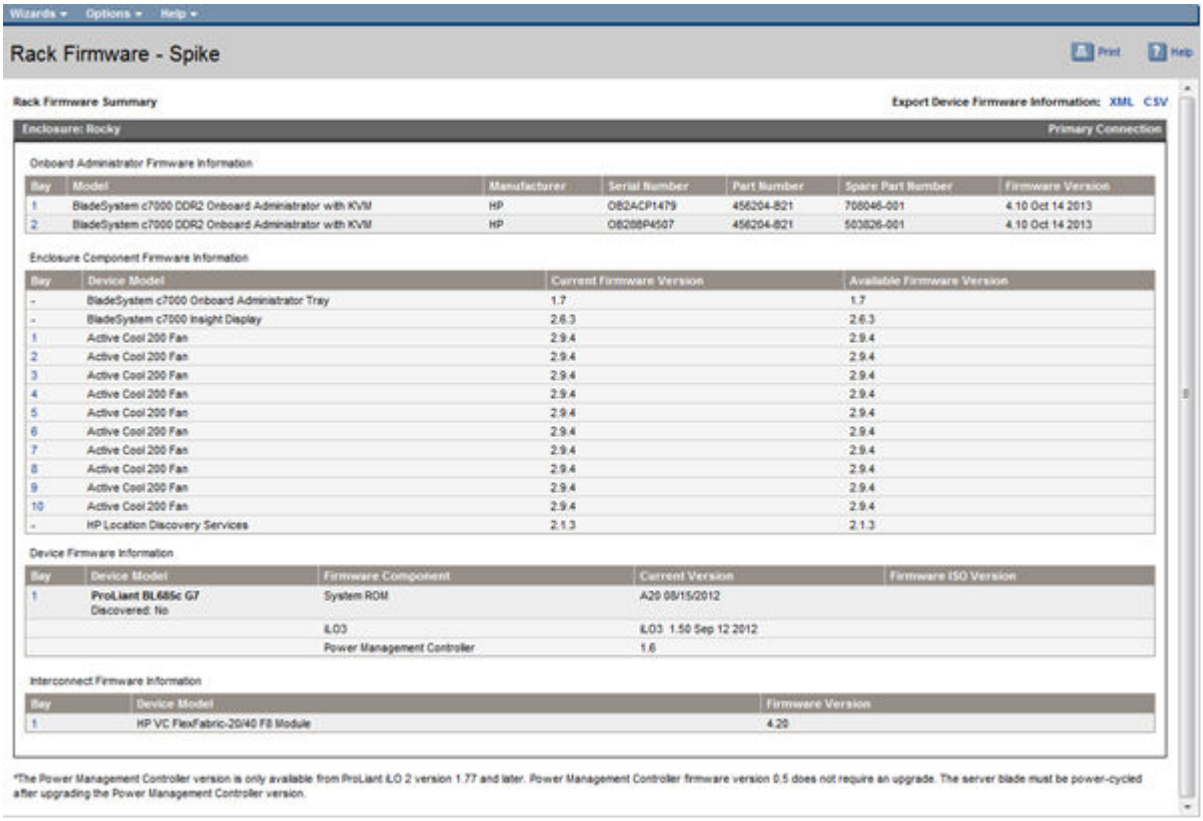
Der Wert für „Present Power“ (Aktueller Verbrauch) stellt den Strom in Watt dar, der von allen Komponenten im Gehäuse verbraucht wird. Die Funktion „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) reguliert automatisch Stromobergrenzen auf Servern im Gehäuse, um Arbeitsauslastungsanforderungen auf Servern zu erfüllen, während gleichzeitig die dynamische Stromobergrenze des Gehäuses eingehalten wird. Der Wert für „Power Limit“ (Strombegrenzung) ist die maximale Menge an Eingangsstrom, die zum Verbrauch durch das Gehäuse verfügbar ist. Dieser Wert ist von der Stromversorgungs-Redundanzeinstellung des Gehäuses und der Anzahl und Position der Netzteile im Gehäuse abhängig. Wurde ein Wert für „Static Power Limit“ (Statische Strombegrenzung) angegeben, zeigt die Strombegrenzung dieses Limit an.

Linked enclosures (Verbundene Gehäuse)

Dieser Abschnitt enthält Informationen für alle verbundenen Gehäuse, an denen Sie angemeldet sind.

Bildschirm „Rack Firmware“ (Rack-Firmware)

„Rack Firmware Summary“ (Übersicht über die Rack-Firmware)


Wizards
Options
Help
Rack Firmware - Spike
Print
Help
Rack Firmware Summary
Export Device Firmware Information: XML CSV
Enclosure: Rocky
Primary Connection
Onboard Administrator Firmware Information
Bay | Model | Manufacturer | Serial Number | Part Number | Spare Part Number | Firmware Version
1 | BladeSystem c7000 DDR2 Onboard Administrator with KVM | HP | OB2ACP1479 | 456204-B21 | 708046-001 | 4.10 Oct 14 2013
2 | BladeSystem c7000 DDR2 Onboard Administrator with KVM | HP | OB2BBP4507 | 456204-B21 | 503826-001 | 4.10 Oct 14 2013
Enclosure Component Firmware Information
Bay | Device Model | Current Firmware Version | Available Firmware Version
- | BladeSystem c7000 Onboard Administrator Tray | 1.7 | 1.7
- | BladeSystem c7000 Insight Display | 2.6.3 | 2.6.3
1 | Active Cool 200 Fan | 2.9.4 | 2.9.4
2 | Active Cool 200 Fan | 2.9.4 | 2.9.4
3 | Active Cool 200 Fan | 2.9.4 | 2.9.4
4 | Active Cool 200 Fan | 2.9.4 | 2.9.4
5 | Active Cool 200 Fan | 2.9.4 | 2.9.4
6 | Active Cool 200 Fan | 2.9.4 | 2.9.4
7 | Active Cool 200 Fan | 2.9.4 | 2.9.4
8 | Active Cool 200 Fan | 2.9.4 | 2.9.4
9 | Active Cool 200 Fan | 2.9.4 | 2.9.4
10 | Active Cool 200 Fan | 2.9.4 | 2.9.4
- | HP Location Discovery Services | 2.1.3 | 2.1.3
Device Firmware Information
Bay | Device Model | Firmware Component | Current Version | Firmware ISO Version
1 | ProLiant BL685c G7 Discovered: No | System ROM | A20 08/15/2012
| | iLO3 | iLO3 1.50 Sep 12 2012
| | Power Management Controller | 1.6
Interconnect Firmware Information
Bay | Device Model | Firmware Version
1 | HP VC FlexFabric-20/40 F8 Module | 4.20
*The Power Management Controller version is only available from ProLiant iLO 2 version 1.77 and later. Power Management Controller firmware version 0.5 does not require an upgrade. The server blade must be power-cycled after upgrading the Power Management Controller version.

HINWEIS: Zur Ansicht kompletter Firmwareversionsinformationen muss mit Enclosure Firmware Management zuerst eine manuelle Ermittlung durchgeführt werden.

Onboard Administrator Firmware information (Informationen zur Onboard Administrator-Firmware)

Spalte	Beschreibung
Bay (Einschub)	Die Nummer des physischen Einschubs, in dem das Onboard Administrator-Modul installiert ist.
Model (Modell)	Die Modellnummer des Onboard Administrator-Moduls.
Manufacturer (Hersteller)	Der Name des Herstellerunternehmens von Onboard Administrator.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Onboard Administrator.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatz-Onboard Administrator-Moduls zu verwendende Teilenummer.
Spare Part Number (Ersatzteilnummer)	Die bei der Bestellung eines zusätzlichen Onboard Administrator oder eines Ersatzgeräts zu verwendende Ersatzteilnummer.
Firmware Version (Firmwareversion)	Die Version des Firmwareimage im Onboard Administrator-Modul.

Enclosure Component Firmware Information (Informationen zur Gehäusekomponenten-Firmware)

Spalte	Beschreibung
Bay (Einschub)	Die Nummer des physischen Einschubs, in dem die Komponente installiert ist.
Device Model (Komponentenmodell)	Die Modellnummer der Komponente.

Spalte	Beschreibung
Current Firmware Version (Aktuelle Firmwareversion)	Die Version der auf der Komponente installierten Firmware.
Available Firmware Version (Verfügbare Firmwareversion)	Die neueste Version der Firmware, die zur Installation auf der Komponente verfügbar ist.

Device Firmware Information (Informationen zur Geräte-Firmware)

Spalte	Beschreibung
Bay (Einschub)	Die Nummer des physischen Einschubs, in dem sich die Komponente im Gehäuse befindet.
Device Model (Komponentenmodell)	Das Modell der Komponente. Das Datum der letzten Firmware-Erkennung wird angezeigt, oder wenn bei der betreffenden Komponente keine Erkennung durchgeführt wurde, wird `No` (Nein) angezeigt.
Firmware Component (Firmwarekomponente)	Der Name der einzelnen Komponenten wird in separaten Zeilen angegeben. Die von der Firmware-DVD unterstützten Komponenten werden aufgeführt, darunter: • System-ROM • iLO • Power Management Controller • NICs • HBAs • Smart Array und angeschlossene Festplattenlaufwerke Bei Komponenten mit mehreren internen Firmwareversionen, wie z. B. NICs, wird jede dieser Versionen separat aufgelistet.
Current Version (Aktuelle Version)	Aktuelle Version der Firmware der betreffenden Komponente.
Firmware DVD Version (Firmware-ISO-Version)	Version der Firmware-DVD der betreffenden Komponente.

Interconnect Firmware information (Informationen zur Verbindungsmodul-Firmware)

Spalte	Beschreibung
Bay (Einschub)	Die Nummer des physischen Einschubs, in dem sich das Verbindungsmodul im Gehäuse befindet.
Device Model (Komponentenmodell)	Das Modell des Verbindungsmoduls.
Firmware Version (Firmwareversion)	Die Firmwareversion des Verbindungsmoduls. `Not Available` (Nicht verfügbar) wird angezeigt, wenn das Verbindungsmodul keine Informationen zur Firmwareversion bereitstellt.

Exportieren von Firmwareinformationen

Um die Informationen zur Firmwareversion, die in diesem Bildschirm angezeigt werden, zum CSV- oder XML-Format zu exportieren, klicken Sie auf **XML** oder **CSV**.

HINWEIS: Die CSV-Option ist nur für Internet Explorer verfügbar.

HINWEIS: Wenn die Blade-Firmware nach der Ermittlung und Aktualisierung eines Servers nicht mit der DVD-ISO-Firmware übereinstimmt, wird ein Informationssymbol angezeigt.

HINWEIS: Ein Buchstabe nach der Firmwareversion bedeutet, dass die Versionshinweise für eine intelligente Komponente überarbeitet wurden. Diese Überarbeitung ist keine funktionelle Firmwareaktualisierung.

8 Konfigurieren von HP BladeSystem-Gehäusen und Gehäusekomponenten

Anzeigen der Statusbildschirme

In der linken Navigationsstruktur kann jedes Gehäuse ausgewählt werden. Wenn Sie auf den Gehäusename klicken, wird die Hauptstatusseite für das zugehörige Gehäuse aufgerufen.

Auf dieser Seite sind oben auf der Hauptseite vier Registerkarten verfügbar: “Status“ (Status), “Information“ (Informationen), “Virtual Buttons“ (virtuelle Schaltflächen) und „Component Firmware“ (Komponentenfirmware).

Auf der Registerkarte „Status“ wird unter „Enclosure Status“ (Gehäusestatus) als allgemeiner Gehäusestatus einer der folgenden Werte angezeigt:

- Critical/Failed (Fehlgeschlagen/Unterbrochen)
- Major (Bedeutende Störung)
- Minor/Degraded (Geringfügige Störung/Beeinträchtigt)
- Normal/OK
- Unknown (Unbekannt)
- Informational (Informativ)

Der Status des aktiven HP BladeSystem Onboard Administrator-Moduls unter „Active OA Status“ und der Status des HP BladeSystem Onboard Administrator-Standby-Moduls unter „Standby OA Status“ sind mit dem allgemeinen Gehäusestatus vergleichbar und zeigen einen Status für Onboard Administrator an. Wenn im System kein Onboard Administrator-Standby-Modul vorhanden ist, wird dies durch den Statuswert „Absent“ (Nicht vorhanden) angegeben.

Unter „Power Mode“ (Stromversorgungsmodus) wird der aktuelle Stromversorgungsmodus des Gehäuses angezeigt. Mögliche Werte sind:

- AC Redundant (Netzredundant)
- Power Supply Redundant (Netzteilredundant)
- Not Redundant (Nicht redundant)

Die Angaben unter „Enclosure Status Overview“ (Gehäusestatus-Übersicht) ist in vier Bereiche unterteilt:

- Device Bay Overview (Übersicht über Geräteeinschübe)
- Interconnect Bay Overview (Übersicht über Verbindungsmoduleinschübe)
- Power Subsystem (Stromversorgungs-Subsystem)
- Thermal Subsystem (Thermisches Subsystem)

Für jede dieser Kategorien sind die folgenden Werte möglich:

- Critical/Failed (Fehlgeschlagen/Unterbrochen)
- Major (Bedeutende Störung)
- Minor/Degraded (Geringfügige Störung/Beeinträchtigt)
- Normal/OK
- Unknown (Unbekannt)
- Informational (Informativ)

Gehäuseeinstellungen

Auswählen von Gehäusen

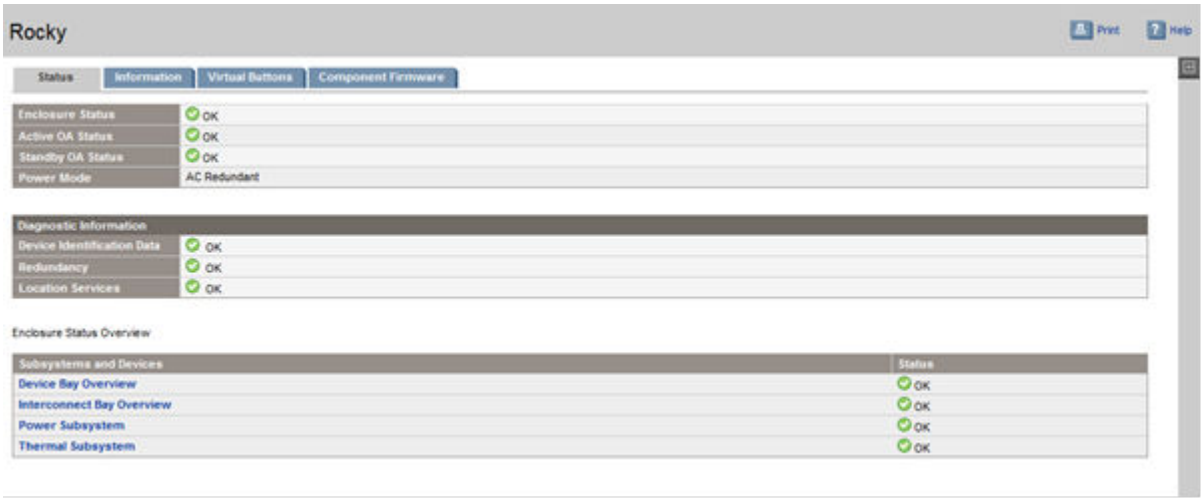
Die Hauptverkettungsports werden in der Tabelle der Rack-Topologie angezeigt. Das Hauptgehäuse ist standardmäßig ausgewählt und seine Auswahl kann nicht aufgehoben werden.

Wenn miteinander verbundene Gehäuse angezeigt werden, ist der von der Anwendung während der Sitzung verwendete Topologie-Modus wie unten beschrieben davon abhängig, welche Kontrollkästchen vor der Anmeldung ausgewählt wurden:

- Modus „Local“ (Lokal): Dies ist der Standard-Topologie-Modus, der aktiviert ist, wenn keines der miteinander verbundenen Gehäuse ausgewählt sind. Alle Topologie-Änderungen, die auftreten, während der Benutzer angemeldet ist, werden von Onboard Administrator ignoriert.
- Modus „Fixed“ (Fest): Dieser Topologie-Modus ist aktiviert, wenn einige, jedoch nicht alle der miteinander verbundenen Gehäuse ausgewählt sind. Die Anwendung zeigt nur die Topologie-Änderungen an, die sich auf die ausgewählten Gehäuse auswirken, während der Benutzer angemeldet ist.
- Modus „Linked“ (Verbunden): Dieser Topololgie-Modus ist aktiviert, wenn alle angezeigten Gehäuse ausgewählt sind. Die Anwendung zeigt alle Topologie-Änderungen an, die auftreten, während der Benutzer angemeldet ist.

Bildschirm „Enclosure Information“ (Gehäuseinformationen)

Um Informationen über das Gehäuse anzuzeigen, wählen Sie **Enclosure Information** (Gehäuseinformationen) aus der Strukturansicht aus. Der Bildschirm „Enclosure Information“ (Gehäuseinformationen) besitzt vier Registerkarten: **Status**, **Information** (Informationen), **Virtual Buttons** (Virtuelle Tasten) und **Component Firmware** (Komponentenfirmware).



Registerkarte „Enclosure Status Overview“ (Gehäusestatusübersicht)

Statusinformationen

Zeile	Beschreibung
Enclosure Status (Gehäusezustand)	Der allgemeine Status des Gehäuses. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt), „N/A“ (Nicht zutreffend) oder „Critical Error“ (Kritischer Fehler).
Active OA Status (Status des aktiven OA)	Der allgemeine Zustand des aktiven Onboard Administrator-Moduls. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Standby OA Status (Status des Standby-OA)	Der allgemeine Zustand des Onboard Administrator Standby-Moduls. Mögliche Werte sind „Absent“ (Nicht vorhanden), „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) oder „Failed“ (Fehler).
Power Mode (Stromversorgungsmodus)	Eine Benutzereinstellung zur Konfiguration der Gleichstromkapazität des Gehäuses und der Redundanz der Stromzufuhr des Gehäuses. Mögliche Werte werden unter „Power-Management“ aufgeführt.

* Der Gehäusestatus wird als „N/A“ (Nicht zutreffend) angezeigt, wenn die Einstellung „Enable Extended Data on GUI Login Page“ (Erweiterte Daten auf GUI-Anmeldeseite aktivieren) deaktiviert ist. Auf diese Einstellung kann über „Enclosure Settings>Network Access>Anonymous Data“ (Gehäuseeinstellungen>Netzwerkzugriff>Anonyme Daten) zugegriffen werden.

Diagnostische Gehäuseinformationen

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

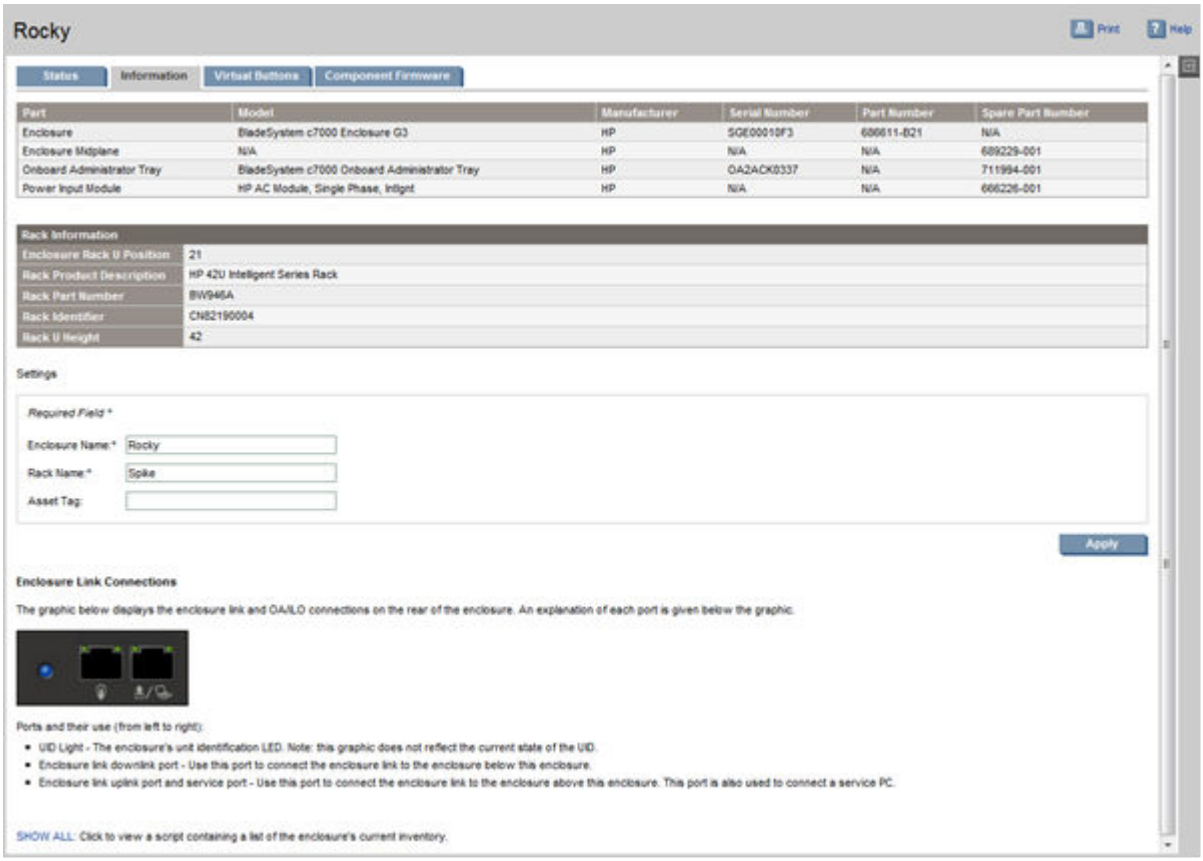
Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Redundancy (Redundanz)	Mögliche Werte sind „OK“ oder „Error“ (Fehler). Ein Fehler weist auf Schwierigkeiten bei der Synchronisierung redundanter Onboard Administrator-Module hin. Überprüfen

Zeile	Beschreibung
	Sie das Systemprotokoll (syslog) auf Fehler. Mögliche Gründe für den Fehler sind unstimmige Firmware- oder Softwareversionen oder ein Hardwareausfall.
Location Services (Positionsdienste)	Mögliche Werte sind „OK“ oder „Other“ (Sonstige). „Other“ (Sonstige) zeigt an, dass ein Fehler für die Positions-Services aufgetreten ist. Möglicherweise wurden Daten beschädigt.

Enclosure Status Overview (Gehäusestatusübersicht)

Subsysteme und Geräte	Beschreibung
Device Bay Overview (Übersicht über Geräteeinschübe)	Der allgemeine Zustand aller Geräteeinschübe. Der Status ist der Gesamtstatus aller Geräte im Gehäuse. Besitzt mehr als ein Gerät einen anderen Status als „OK“, dann werden sie in dieser Tabelle aufgelistet.
Interconnect Bay Overview (Übersicht über Verbindungsmoduleinschübe)	Der allgemeine Zustand der Verbindungsmoduleinschübe. Der Status ist der Gesamtstatus aller Verbindungsmodule im Gehäuse. Besitzt mehr als ein Verbindungsmodul einen anderen Status als „OK“, dann werden sie in dieser Tabelle aufgelistet.
Power Subsystem (Stromversorgungs-Subsystem)	Der allgemeine Zustand des Stromversorgungs-Subsystems des Gehäuses. Der Status ist der Gesamtstatus aller Netzteile im Gehäuse. Besitzt mehr als ein Netzteil einen anderen Status als „OK“, dann werden sie in dieser Tabelle aufgelistet.
Thermal Subsystem (Thermisches Subsystem)	Der allgemeine Status des thermischen Subsystems des Gehäuses. Der Status ist der Gesamtstatus aller Lüfter im Gehäuse. Besitzt mehr als ein Lüfter einen anderen Status als „OK“, dann werden sie in dieser Tabelle aufgelistet.

Registerkarte „Enclosure Information“ (Gehäuseinformationen)



Hardwareinformationen

Spalte	Beschreibung
Part (Teil)	Der Name des Teils.
Model (Modell)	Die Modellnummer des Teils.
Manufacturer (Hersteller)	Der Name des Herstellerunternehmens des Teils.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Teils.
Part Number (Artikelnummer)	Die Teilenummer für die Bestellung eines zusätzlichen Teils. Da das „Power Input Module“ (Netzeingangsmodul) keine Teilenummer besitzt, wird in der Spalte „Part Number“ (Teilenummer) immer „N/A“ angezeigt.
Spare Part Number (Ersatzteilnummer)	Die Teilenummer für die Bestellung eines Ersatzteiles.

Rack-Informationen

Zeile	Beschreibung
Enclosure Rack U Position (Rack-U-Position des Gehäuses)	Die Position des Gehäuses im Rack.
Rack Product Description (Rack-Produkt-Beschreibung)	Der allgemeine beschreibende Name des Racks.
Rack Part Number (Rack-Teilenummer)	Die Teilenummer für die Bestellung eines Ersatz-Racks.

Zeile	Beschreibung
Rack Identifier (Rack-Kennung)	Eine eindeutige Zeichenfolge, anhand der das Rack identifiziert wird.
Rack U Height (Rack-U-Höhe)	Die U-Höhe des Racks.

Dazu gehören die von den Positionsermittlungsdiensten (Location Discovery Services) erfassten Informationen. Weitere Informationen zur Verwendung von Positionsermittlungsdiensten (Location Discovery Services) finden Sie unter „Bildschirm ‚Rack Overview' (Rack-Übersicht)" (Bildschirm „Rack Overview" (Rack-Übersicht) auf Seite 100).

Ändern der Einstellungen

Die Gehäuseeinstellungen können in diesem Bildschirm geändert werden. Um die Einstellungen nach der Vornahme von Änderungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Feld	Möglicher Wert	Beschreibung
Enclosure Name (Gehäusename)	1 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Der Name des ausgewählten Gehäuses.
Rack Name (Rack-Name)	1 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Der Name des Racks, in dem das Gehäuse installiert ist.
Asset Tag (Systemkennung)	0 bis 32 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Die Systemkennung wird zur Bestandskontrolle verwendet. Die Standardsystemkennung ist leer.

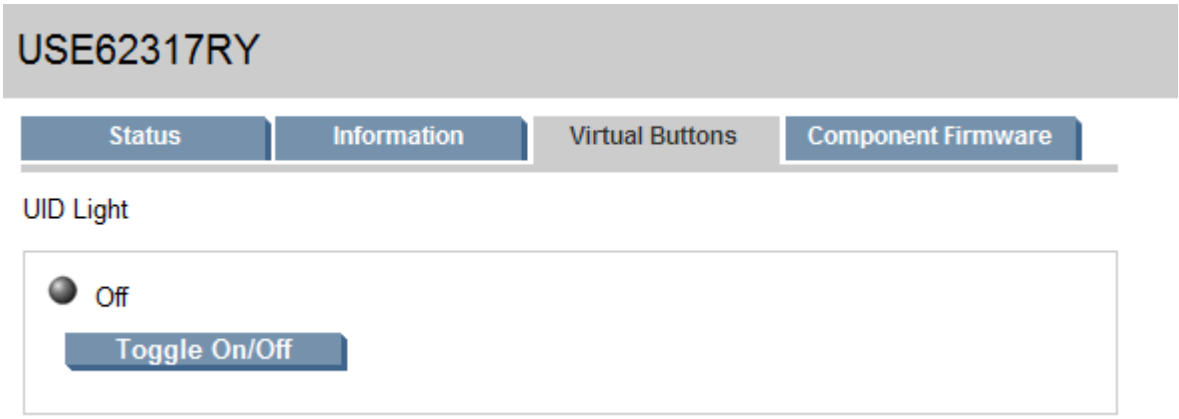
„Enclosure Link Connections" (Gehäuse-Verbindungsanschlüsse)

In diesem Abschnitt wird eine grafische Ansicht der Gehäuse-Verbindungsanschlüsse bereitgestellt, die sich an der Rückseite des Gehäuses befinden. Außerdem erhalten Sie detaillierte Informationen zu den einzelnen Gehäuse-Verbindungsports.

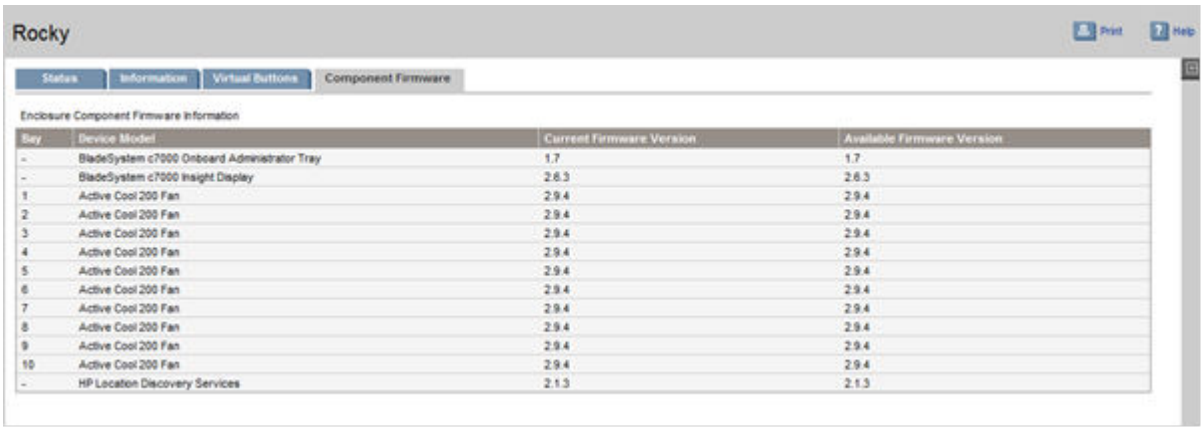
Um ein Skript anzuzeigen, das die Liste des aktuellen Bestands des Gehäuses enthält, klicken Sie auf **SHOW ALL** (ALLES ANZEIGEN).

Virtuelle Tasten

Um den Zustand der Gehäuse-UID-LED zu ändern, die sich neben den Gehäuse-Link- und Onboard Administrator/iLO-Anschlüssen befindet, klicken Sie auf **Toggle On/Off** (Ein-/Ausschalten).



Komponenten-Firmware


Rocky
Print
Help
Status
Information
Virtual Buttons
Component Firmware
Enclosure Component Firmware Information
Bay
Device Model
Current Firmware Version
Available Firmware Version
- BladeSystem c7000 Onboard Administrator Tray 1.7 1.7
- BladeSystem c7000 Insight Display 2.6.3 2.6.3
1 Active Cool 200 Fan 2.9.4 2.9.4
2 Active Cool 200 Fan 2.9.4 2.9.4
3 Active Cool 200 Fan 2.9.4 2.9.4
4 Active Cool 200 Fan 2.9.4 2.9.4
5 Active Cool 200 Fan 2.9.4 2.9.4
6 Active Cool 200 Fan 2.9.4 2.9.4
7 Active Cool 200 Fan 2.9.4 2.9.4
8 Active Cool 200 Fan 2.9.4 2.9.4
9 Active Cool 200 Fan 2.9.4 2.9.4
10 Active Cool 200 Fan 2.9.4 2.9.4
- HP Location Discovery Services 2.1.3 2.1.3

Spalte	Beschreibung
Bay (Einschub)	Der Geräteeinschub innerhalb des Gehäuses.
Device Model (Komponentenmodell)	Die Modellnummer der Komponente.
Current Firmware Version (Aktuelle Firmwareversion)	Die installierte Firmwareversion der Komponente.
Available Firmware Version (Verfügbare Firmwareversion)	Die neueste Version der derzeit für die Komponente verfügbaren Firmware.

Die Registerkarte „Enclosure Component Firmware“ (Gehäusekomponenten-Firmware) zeigt auch die Firmwareversion des Positions-PIC (BladeSystem-Positionsgerät), die von den Positionsermittlungsdiensten (Location Discovery Services) bereitgestellt wird. Weitere Informationen zur Verwendung von Positionsermittlungsdiensten (Location Discovery Services) finden Sie unter „Bildschirm ‚Rack Overview‘ (Rack-Übersicht)“ (Bildschirm „Rack Overview“ (Rack-Übersicht) auf Seite 100).

AlertMail

Mit AlertMail können Benutzer per E-Mail anstatt mithilfe von SNMP-Traps über Systemereignisse informiert werden. AlertMail ist vollkommen unabhängig von SNMP. Beide Optionen können gleichzeitig aktiviert sein. AlertMail verwendet für die Kommunikation mit einem SMTP-fähigen Mailserver SMTP-Standardbefehle. Die Antwortadresse für jede von AlertMail gesendete E-Mail

lautet <Gehäusename>@<Domäne des Mitteilungsabsenders>. Um die AlertMail-Funktion zu aktivieren, markieren Sie das Kontrollkästchen **Enable AlertMail** (AlertMail aktivieren).

Um die AlertMail-Funktion zu testen, vergewissern Sie sich, dass die E-Mail-Adresse, die Domäne des Mitteilungssenders und die SMTP-Servereinstellungen korrekt sind. Wählen Sie **Send Test AlertMail** (Test-AlertMail senden). Um zu bestätigen, dass der Test erfolgreich ausgeführt wurde, überprüfen Sie das E-Mail-Konto des Empfängers.

HINWEIS: Unter Umständen wird die Angabe „Alert Sender Domain“ (Domäne des Mitteilungsabsenders) nicht benötigt. Dieses Feld hängt von der Einrichtung des E-Mail-Servers ab.

Feld	Möglicher Wert	Beschreibung
E-Mail Address (E-Mail-Adresse)	<Konto>@<Domäne>	Eine gültige E-Mail-Adresse für den Administrator oder eine andere für den Empfang der E-Mail-Benachrichtigung berechtigte Person.
SMTP Server (SMTP-Server)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-).	Eine IPv4-Adresse, IPv6-Adresse oder der DNS-Name für den SMTP-Server.
Alert Sender Name (Name des Mitteilungsabsenders)	Eine Zeichenfolge, die alle alphanumerischen Zeichen, den Bindestrich (-), den Unterstrich (_) und Leerzeichen enthalten kann. Das Feld ist optional und auf 40 Zeichen begrenzt.	Onboard Administrator Name

Feld	Möglicher Wert	Beschreibung
Alert Sender Domain (Domäne des Mitteilungsabsenders)	Eine Zeichenfolge, die sämtliche alphanumerischen Zeichen, den Bindestrich (-) und den Punkt (.) enthalten kann.	Die Domäne, in der sich Onboard Administrator befindet. Sich gegenseitig ausschließend mit der Absender-E-Mail.
Alert Sender E-mail (E-Mail des Mitteilungsabsenders)	<Konto>@<Domäne>	Die gültige E-Mail-Adresse des Absenders für den Administrator oder eine andere für den Empfang der E-Mail-Benachrichtigung berechtigte Person.

1. Markieren Sie das Kontrollkästchen **Enable AlertMail** (AlertMail aktivieren), um die Funktion „AlertMail“ zu aktivieren.
2. Geben Sie die Werte für die E-Mail-Adresse, die Domäne des Mitteilungsabsenders und den SMTP-Server ein.
3. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Bei aktivierter Option sendet AlertMail eine E-Mail beim Eintreten der folgenden Ereignisse:

- Änderung des Gehäusestatus
- Änderung der Gehäuseinformationen
- Änderung des Lüfterstatus
- Lüftereinbau
- Lüfterausbau
- Netzteilstatus
- Netzteileinbau
- Netzteilausbau
- Netzteilüberlastung
- Blade-Einbau
- Blade-Ausbau
- Blade-Status
- Wärmezustand des Blade
- Blade-Störung
- Änderung der Blade-Informationen
- Änderung des Fachstatus
- Zurücksetzen von Fächern
- Switch-Verbindung
- Switch-Trennung

Alle E-Mails besitzen den folgenden Header:

```
Von: Enclosure GEHÄUSENAME <Gehäusename@Serverdomäne>
```

```
Datum: Datum im Standardformat

Betreff: HP AlertMail-SEQ: <SCHWEREGRAD> THEMA

An: RECEIVER MAILBOX (POSTFACH DES EMPFÄNGERS)
```

Der SCHWEREGRAD wird mithilfe eines der folgenden Werte ausgedrückt (vom höchsten Wert absteigend):

- # FATAL (Nicht behebbarer Fehler)
- # CRITICAL (Kritischer Fehler)
- # WARNING MAJOR (Schwerwiegender Fehler)
- # WARNING MINOR (Geringfügiger Fehler)
- # WARNING (Warnung)
- # NORMAL (Normalzustand)

Jede Betreffzeile enthält eine eindeutige fortlaufende Nummer zur Identifizierung der Ereignisreihenfolge, falls der Mailserver die Ereignisse in der falschen Reihenfolge verteilt. Als fortlaufende Nummern werden 0 bis 999 verwendet. Nach Erreichen der letzten verfügbaren Nummer beginnt die Zählung wieder bei 0.

Der Textteil der E-Mail enthält detaillierte Informationen zu dem betreffenden Ereignis. Er kann auch Empfehlungen für korrigierende Maßnahmen sowie Angaben zum aktuellen Gehäusestatus umfassen.

HINWEIS: Der Gehäusestatus wird als Status zum Zeitpunkt der Ereignisverarbeitung angezeigt. Das kann dazu führen, das der Status in einer E-Mail als OK bezeichnet wird, die einen Lüfterausfall meldet, wenn der Benutzer den Lüfter bereits ausgetauscht hat, als die Ereignismitteilung von AlertMail gesendet wurde.

Beispiel für eine E-Mail:

```
Betreff: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed (HP-
Benachrichtigungs-E-Mail 010: (KRITISCH) Netzteil #1: Fehler)

Datum: Wed, 23 Apr 2006 15:02:22 +0200 (Mittwoch, 23. April 2006,
15:02:22 +0200)

Betreff: Enclosure EM-00508BEBA571 EM-00508BEBA571@hp.com (Gehäuse
EM-00508BEBA571 EM-00508BEBA571@hp.com)

An: Benutzer@Domäne

X-OS: HP BladeSystem Enclosure Manager

X-Priority: 1

Content-Type: text/plain; charset=us-ascii


EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed
(EREIGNIS (26. Mai, 07:09): Netzteil #1 Status geändert zu: Fehler)


Enclosure, EM-00508BEBA571, has detected that a power supply in bay 1 has
changed from status OK to Failed. (Gehäuse EM-00508BEBA571 hat erkannt,
dass sich der Status eines Netzteils in Einschub 1 von „OK“ in „Failed“
geändert hat.)
```

The power supply should be replaced with the appropriate spare part. (Das Netzteil sollte gegen ein passendes Ersatzteil ausgetauscht werden.) You can ensure that the center wall assembly is operating correctly by swapping the two power supplies. (Sie können sicherstellen, dass die Baugruppe der mittleren Wand korrekt funktioniert, indem Sie die beiden Netzteile vertauschen.) Make sure that there are no bent pins on the power supply connectors before reinserting and that each power supply is fully seated. (Vergewissern Sie sich vor der Montage, dass die Netzteilanschlüsse keine verbogenen Kontaktstifte aufweisen und dass alle Netzteile fest sitzen.)

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power has occurred. (Eine gelbe LED-Anzeige am Netzteil weist auf eine Überspannung, das Überschreiten des Temperaturgrenzwerts oder den Verlust der Netzversorgung hin.) A blinking LED on the power supply indicates a current limit condition. (Eine blinkende LED-Anzeige am Netzteil gibt einen aktuellen Zustand im Grenzbereich an.)

Enclosure Status: Degraded (Gehäusestatus: Degraded (Beeinträchtigt))

Enclosure Management URL: https://16.181.75.213/ (Gehäuse-Management-URL: https://16.181.75.213/)

- PLEASE DO NOT REPLY TO THIS EMAIL -

Registerkarten „Device Power Sequence Device Bays“ (Komponenten-Startsequenz der Geräteeinschübe)

Die Stromzufuhrverzögerungsfunktion des Gehäuses steuert die Reihenfolge, in der Komponenten eingeschaltet werden, wenn das gesamte Gehäuse aus- und wieder eingeschaltet wurde. Diese Funktion ist nur während des Boot-Vorgangs des aktiven HP BladeSystem-Onboard Administrator-Moduls aktiviert, wenn Onboard Administrator erkennt, dass das gesamte Gehäuse aus- und wieder eingeschaltet und die Stromzufuhrverzögerung auf mindestens einer Komponente im Gehäuse aktiviert wurde.

Der aktive HP BladeSystem-Onboard Administrator zeigt im Systemprotokoll eine Meldung an, wenn die Stromzufuhrverzögerung gestartet wurde und auch wenn die Stromzufuhrverzögerung beendet wurde, nachdem die längste Stromzufuhrverzögerung verstrichen ist. Der HP BladeSystem-Onboard Administrator ist ab Werk so eingestellt, dass die Stromzufuhrverzögerung für alle Komponenten deaktiviert wird.

Typische Anwendungsfälle für Abhängigkeiten zwischen Einschüben, die durch Aktivieren der Stromzufuhrverzögerungsfunktion des Gehäuses aufgelöst werden können, sind:

- **Boot from network (Über das Netzwerk starten)**: Netzwerkverbindungsmodule müssen vor Servern, die für einen Netzwerkstart konfiguriert sind (z. B. PXE oder iSCSI), einen Selbsttest beim Systemstart durchführen.
- **Boot from SAN (Über SAN starten)**: SAN-Verbindungsmodule müssen vor Servern, die für einen SAN-Start konfiguriert sind, einen Selbsttest beim Systemstart durchführen.
- Wichtige Service-Abhängigkeiten, die von einem Server gesteuert werden, z. B. DHCP oder Lizenzierung.
- Speicherserver müssen vor Servern betriebsbereit sein, die diese Ressourcen benötigen.

Die Einstellung der Verzögerungsdauer muss empirisch bestimmt werden, da sich einige Abhängigkeiten außerhalb des Gehäuses befinden (der Start über SAN könnte eine zusätzliche Verzögerung erforderlich machen, damit das SAN-Speichersystem des Datenzentrums eingeschaltet werden kann). Für jedes Verbindungsmodul gilt eine andere Einschalt-Zeiteinstellung, bevor es betriebsbereit ist.

Der für die Stromzufuhrverzögerung verwendete Zeitgeber wird gestartet, wenn der Onboard Administrator die erste Systemprotokollmeldung während der Onboard Administrator-Initialisierung einträgt. Dies wird durch die Systemprotokollmeldung `Kernel: Network link up` (Kernel: Netzwerk-Link-up) angegeben. Wenn der HP BladeSystem-Onboard Administrator im Systemprotokoll die Meldung `PowerDelay has been initiated for the selected devices` (Stromzufuhrverzögerung wurde für die ausgewählten Komponenten gestartet) angibt, wird die konfigurierte Verzögerungsdauer für jeden Einschub verwendet, um festzulegen, wann die betreffende Komponente eingeschaltet wird. Nachdem die ausgewählte Verzögerungsdauer verstrichen ist, wird die Komponente eingeschaltet.

Gültige Einstellungen für die einzelnen Einschübe sind: „Disabled“ (Deaktiviert), „Enabled“ (Aktiviert) und „No Poweron“ (Kein Einschalten).

Disabled (Deaktiviert): Deaktiviert die Stromzufuhrverzögerung für diesen Einschub. HP BladeSystem Onboard Administrator führt diesem Einschub Strom auf der Basis der Energieeinstellungen zu: Im Fall eines Geräts, das für die automatische Einschaltung konfiguriert wurde, wird dem Gerät Strom im Anschluss an das Aus- und Wiedereinschalten des Gehäuses zugeführt, nachdem alle Onboard Administrator-Konfigurationsprüfungen abgeschlossen sind.

Enabled (Aktiviert): Aktiviert die Stromzufuhrverzögerung für diesen Einschub. HP BladeSystem-Onboard Administrator schaltet diesen Einschub entsprechend der Anzahl der Sekunden ein, die verstrichen sind, nachdem das Aus- und Wiedereinschalten des Gehäuses erkannt wurde.

No Poweron (Kein Einschalten): Verhindert das Einschalten von Komponenten für die Einschübe mit dieser Konfiguration, bis der HP BladeSystem Onboard Administrator die Meldung `PowerDelay has completed for the selected devices` (Stromzufuhrverzögerung wurde für die ausgewählten Komponenten abgeschlossen) ausgibt. Wenn die Komponente für automatisches Einschalten konfiguriert ist, gewährt die Komponente jetzt die Stromzufuhr nach dem Aus- und Wiedereinschalten des Gehäuses, nachdem alle Onboard Administrator-Konfigurationsprüfungen abgeschlossen wurden.

Wenn die Komponente so konfiguriert ist, dass automatisches Einschalten deaktiviert ist, bleibt die Komponente unabhängig von der Einstellung für die Stromzufuhrverzögerung nach dem Aus- und Wiedereinschalten des Gehäuses ausgeschaltet.

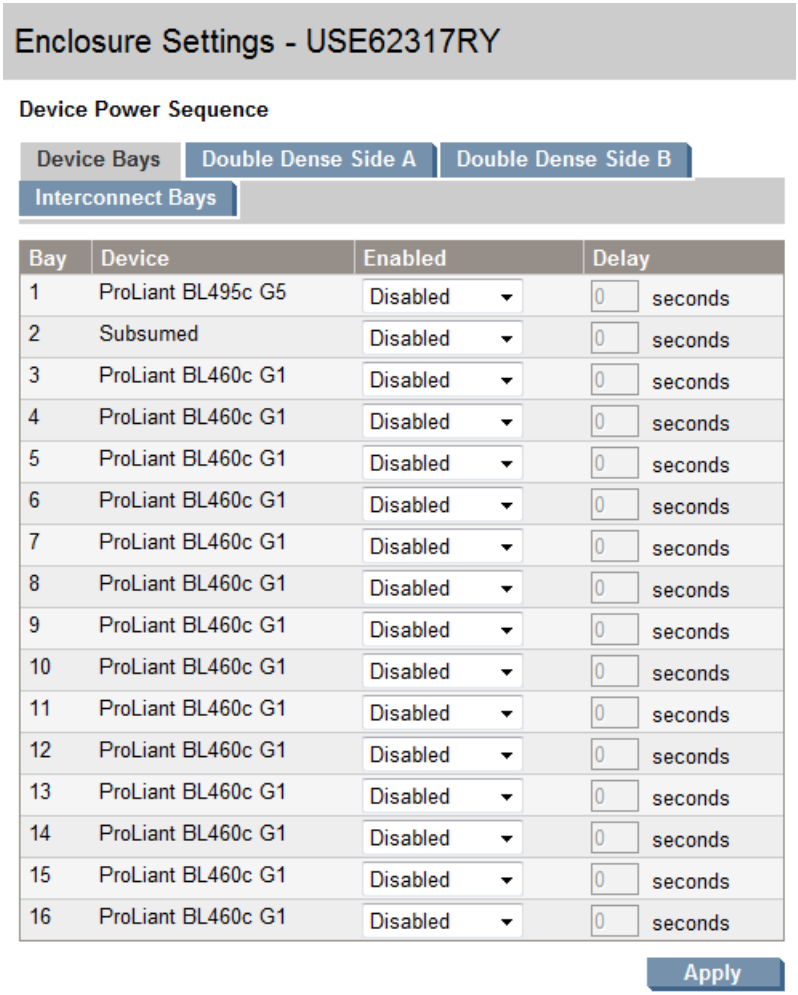
Standardregisterkarte und Registerkarten doppelter Dichte der Geräteeinschübe

Die Registerkarte „Device Bays Standard“ (Geräteeinschübe Standard) gibt die aktuellen Einstellungen für alle primären Einschübe anhand des Gehäusetyps an. Um eine Einstellung für einen bestimmten Geräteeinschub zu ändern, verwenden Sie das Menü unter der Spalte „Enabled“ (Aktiviert), und wählen Sie die Option „Enabled“ (Aktiviert), „Disabled“ (Deaktiviert) oder „No Poweron“ (Kein Einschalten). Bei Auswahl von „Enabled“ (Aktiviert) muss in die Spalte „Delay“ (Verzögerung) eine Stromzufuhrverzögerung in Sekunden für diesen Einschub eingetragen werden. Der Mindestwert ist 1 Sekunde; der Höchstwert ist 3600 Sekunden.

Wenn Server doppelter Dichte in einem Gehäuse installiert sind, werden die Stromzufuhrverzögerungseinstellungen für Seite A und Seite B auf den Registerkarten „Double Dense Side A“ (Doppelte Dichte Seite A) und „Double Dense Side B“ (Doppelte Dichte Seite B) gesteuert.

Registerkarte „Interconnect Bays“ (Verbindungsmoduleinschübe)

Verbindungsmoduleinschübe sind standardmäßig auf automatisches Einschalten eingestellt. Das Aktivieren und Festlegen einer Stromzufuhrverzögerung für einen Verbindungsmoduleinschub verzögert das Einschalten für diesen Einschub nach dem Aus- und Wiedereinschalten des Gehäuses.


Enclosure Settings - USE62317RY
Device Power Sequence
Device Bays
Double Dense Side A
Double Dense Side B
Interconnect Bays
Bay
Device
Enabled
Delay
1 ProLiant BL495c G5 Disabled 0 seconds
2 Subsumed Disabled 0 seconds
3 ProLiant BL460c G1 Disabled 0 seconds
4 ProLiant BL460c G1 Disabled 0 seconds
5 ProLiant BL460c G1 Disabled 0 seconds
6 ProLiant BL460c G1 Disabled 0 seconds
7 ProLiant BL460c G1 Disabled 0 seconds
8 ProLiant BL460c G1 Disabled 0 seconds
9 ProLiant BL460c G1 Disabled 0 seconds
10 ProLiant BL460c G1 Disabled 0 seconds
11 ProLiant BL460c G1 Disabled 0 seconds
12 ProLiant BL460c G1 Disabled 0 seconds
13 ProLiant BL460c G1 Disabled 0 seconds
14 ProLiant BL460c G1 Disabled 0 seconds
15 ProLiant BL460c G1 Disabled 0 seconds
16 ProLiant BL460c G1 Disabled 0 seconds
Apply

Spalte	Beschreibung
Bay (Einschub)	Einschubnummer der Komponente.
Device (Gerät)	Die Art von Komponente im Einschub, oder „Absent“ (Nicht vorhanden), wenn im Einschub keine Komponente installiert ist.
Enabled (Aktiviert)	Aktiviert die Startsequenz, deaktiviert die Startsequenz oder gestattet nicht das Einschalten der Komponente, wenn „No Poweron“ (Kein Einschalten) ausgewählt ist.
Delay (Verzögerung)	Die Verzögerung in Sekunden, bevor die Komponente eingeschaltet wird.

Registerkarte „Device Power Sequence Interconnect Bays“ (Komponenten-Startsequenz der Verbindungsmoduleinschübe)

Spalte	Beschreibung
Bay (Einschub)	Einschubnummer der Komponente.
Device (Gerät)	Die Art von Komponente im Einschub oder „Absent“ (Nicht vorhanden), wenn im Einschub keine Komponente installiert ist.
Enabled (Aktiviert)	Aktiviert die Startsequenz, deaktiviert die Startsequenz oder gestattet nicht das Einschalten der Komponente, wenn „No Poweron“ (Kein Einschalten) ausgewählt ist.
Delay (Verzögerung)	Die Verzögerung in Sekunden, bevor die Komponente eingeschaltet wird. Mögliche Verzögerungswerte sind 1 bis 3600.

Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Datum und Uhrzeit

Statische Datums- und Uhrzeiteinstellungen

Datum und Uhrzeit sind statisch und werden nicht in Echtzeit aktualisiert. Datum und Uhrzeit können nur eingestellt werden, wenn NTP deaktiviert ist.

Feld	Möglicher Wert	Beschreibung
Date (Datum)	JJJJ-MM-TT • MM ist eine ganze Zahl von 1 bis 12 • TT ist eine ganze Zahl von 1 bis 31	Das Datum, das dem Gehäuse zugewiesen wurde.
Time (Uhrzeit)	HH:MM:SS (24-Stunden-Format, SS ist optional) • HH ist eine ganze Zahl von 0 bis 23 • MM ist eine ganze Zahl von 0 bis 59	Die Uhrzeit, die dem Gehäuse zugewiesen wurde.
Time Zone (Zeitzone)	Zeitzoneneinstellungen • Zeitzoneneinstellungen für Afrika (Zeitzoneneinstellungen für Afrika auf Seite 428) • Zeitzoneneinstellungen für Amerika (Zeitzoneneinstellungen für Amerika auf Seite 429) • Zeitzoneneinstellungen für Asien (Zeitzoneneinstellungen für Asien auf Seite 431)	Die aktuelle Zeitzone, die dem Gehäuse zugeordnet wurde.

Feld	Möglicher Wert	Beschreibung
	• Zeitzoneneinstellungen für die Universalzeit (Zeitzoneneinstellungen für die Universalzeit auf Seite 428) • Zeitzoneneinstellungen für Ozeanien (Zeitzoneneinstellungen für Ozeanien auf Seite 432) • Zeitzoneneinstellungen für Europa (Zeitzoneneinstellungen für Europa auf Seite 433) • Zeitzoneneinstellungen für Polar-Zeit (Zeitzoneneinstellungen für Polar-Zeit auf Seite 433)	

NTP-Einstellungen

Um diese Funktion zu aktivieren, wählen Sie **Set time using an NTP server** (Uhrzeit über einen NTP-Server einstellen).

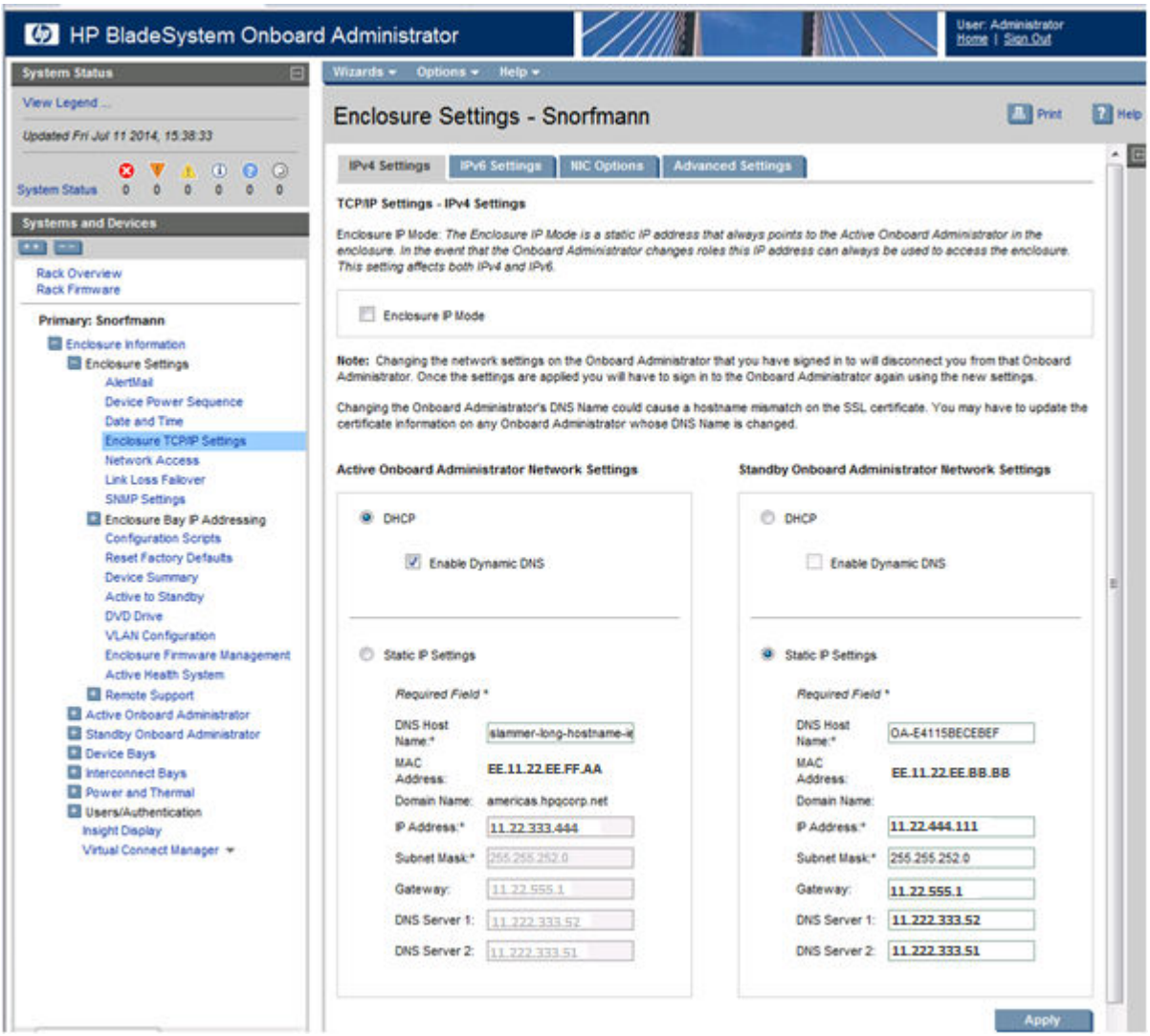
Feld	Möglicher Wert	Beschreibung
Primary NTP Server (Primärer WINS-Server)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:###:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-).	IP-Adresse oder DNS-Name des primären NTP-Servers, der Datums- und Uhrzeitinformationen liefert.
Secondary NTP Server (Sekundärer WINS-Server)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:###:####:####:####:####, wobei #### im	IP-Adresse oder DNS-Name des sekundären NTP-Servers, der Datums- und Uhrzeitinformationen liefert.

Feld	Möglicher Wert	Beschreibung
	Bereich von 0 bis FFFF liegt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-).	
Poll Interval (Abfrageintervall)	Eine ganze Zahl von 60 bis 86400	Hierbei handelt es sich um das Intervall, in dem der NTP-Server abgefragt wird (Angabe in Sekunden).
Time Zone (Zeitzone)	Zeitzoneneinstellungen • Zeitzoneneinstellungen für Afrika (Zeitzoneneinstellungen für Afrika auf Seite 428) • Zeitzoneneinstellungen für Amerika (Zeitzoneneinstellungen für Amerika auf Seite 429) • Zeitzoneneinstellungen für Asien (Zeitzoneneinstellungen für Asien auf Seite 431) • Zeitzoneneinstellungen für die Universalzeit (Zeitzoneneinstellungen für die Universalzeit auf Seite 428) • Zeitzoneneinstellungen für Ozeanien (Zeitzoneneinstellungen für Ozeanien auf Seite 432) • Zeitzoneneinstellungen für Europa (Zeitzoneneinstellungen für Europa auf Seite 433) • Zeitzoneneinstellungen für Polar-Zeit (Zeitzoneneinstellungen für Polar-Zeit auf Seite 433)	Die aktuelle Zeitzone, die dem Gehäuse zugeordnet wurde.

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen)

Registerkarte „IPv4-Einstellungen“



Registerkarte „IPv4-Einstellungen“

Enclosure IP Mode (Gehäuse-IP-Modus)

Wenn die Einstellung **Enclosure IP Mode** (Gehäuse-IP-Modus) aktiviert ist, wird mit ihr sichergestellt, dass alle Verwaltungsanwendungen mittels einer einzelnen statischen IP-Adresse auf das aktive Onboard Administrator-Modul des Gehäuses verweisen. Dieser Modus ist für Gehäuse mit einem aktiven und einem Onboard Administrator Standby-Modul bestimmt. Wenn das Onboard Administrator Standby-Modul die Rolle des aktiven Onboard Administrator-Moduls übernimmt, übernimmt das betreffende Onboard Administrator-Modul die IP-Adresse des vorherigen aktiven Onboard Administrator-Moduls. Dieser Modus stellt sicher, dass die IP-Adresse von „Enclosure IP Mode“ (Gehäuse-IP-Modus) ständig auf das aktive Onboard Administrator-Modul verweist.

Für den **Enclosure IP Mode** (Gehäuse-IP-Modus) muss der aktive Onboard Administrator über eine statische IPv4- oder eine statische IPv6-Adresse verfügen (IPv6 muss aktiviert sein). Das Onboard Administrator Standby-Modul kann für DHCP oder statische IP-Einstellungen konfiguriert werden. Dieser Modus ist optional und standardmäßig deaktiviert.

Um sicherzustellen, dass die Einstellung „Enclosure IP Mode“ (Gehäuse-IP-Modus) beim Entfernen eines Onboard Administrator-Moduls aus dem Gehäuse nicht geändert wird, darf das Modul nicht in der Failover-Übergangsphase (etwa sechs Minuten nach einem Failover) entfernt werden. Um nach dem Entfernen eines Moduls sicherzustellen, dass alle Einstellungen auf das Standby-Modul übertragen werden, fügen Sie ein Ersatzmodul hinzu und lassen Sie fünf Minuten lang angeschlossen. Sollten das aktive und das Standby-Onboard Administrator-Modul gleichzeitig ausgeschaltet oder aus dem Gehäuse entfernt werden, wird das Standby-Onboard Administrator-Modul auf die Standardnetzwerkeinstellungen zurückgesetzt und alle manuell konfigurierten statischen Netzwerkadressen gehen verloren.

HINWEIS: Diese Funktion ist im FIPS-Modus ON/DEBUG deaktiviert.

HINWEIS: Wenn **Enclosure IP Mode** (Gehäuse-IP-Modus) auf der Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) oder auf der Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) aktiviert wird, wird dieser Modus automatisch auf beiden Registerkarten aktiviert.

Netzwerkeinstellungen des aktiven und des Standby-Onboard Administrator-Moduls

In Onboard Administrator kann die IPv4-Netzwerkkonfiguration entweder auf dynamisch zugewiesenen IP-Adressen basieren, die von einem DHCP-Server bezogen wurden, oder auf statischen IP-Adressen, die von Ihnen manuell angegeben wurden. Sie wählen die Grundlagen für die Netzwerkkonfiguration aus, indem Sie entweder das Optionsfeld **DHCP** oder das Optionsfeld **Static IP Settings** (Statische IP-Einstellungen) aktivieren. Bei der Auswahl von **DHCP** kann „Dynamic DNS“ (Dynamisches DNS) aktiviert werden.

HINWEIS: Bei einer Änderung der Netzwerkeinstellungen auf dem Onboard Administrator, bei dem Sie angemeldet sind, wird Ihre Verbindung mit dem Onboard Administrator möglicherweise getrennt. In diesem Fall müssen Sie sich nach dem Anwenden der Einstellungen wieder bei dem Onboard Administrator anmelden.

- **DHCP**: Bezieht die IP-Adresse für Onboard Administrator von einem DHCP-Server.
- **Enable Dynamic DNS** (Dynamisches DNS aktivieren): Wenn DHCP aktiviert ist, ermöglicht „Dynamic DNS“ (Dynamisches DNS) die Verwendung des gleichen Hostnamens für den Onboard Administrator über eine Zeitspanne hinweg, obwohl sich die dynamisch zugewiesene IP-Adresse ändern könnte. Der Hostname wird bei einem DNS-Server registriert. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Aufzeichnungen für IP-Adressen.

  Wenn „Dynamic DNS“ (Dynamisches DNS) auf Onboard Administrator deaktiviert wird, werden die Onboard Administrator-Aktualisierungen am DNS-Server gestoppt. Es ist jedoch zu beachten, dass bei einigen DHCP-Servern eine Regelung die direkte Aktualisierung von DNS-Servern ermöglicht. Um dynamische DNS-Aktualisierungen vollständig zu deaktivieren, müssen Sie „Dynamic DNS“ (Dynamisches DNS) sowohl auf dem Onboard Administrator als auch auf dem DHCP-Server deaktivieren.
- **Static IP Settings** (Statische IP-Einstellungen): Ermöglicht das manuelle Einrichten statischer IP-Einstellungen für den Onboard Administrator.

ACHTUNG: Wenn DHCP für IPv4 aktiviert wird, gehen alle statischen IPv4-Einstellungen verloren.

Feld	Möglicher Wert	Beschreibung
DNS Host Name (DNS-Hostname)	Kann 1 bis 32 Zeichen umfassen, einschließlich aller alphanumerischen	Der DNS-Name des Onboard Administrator-Moduls. Diese Einstellung gilt für IPv4- und IPv6-Umgebungen. Der DNS-Hostname kann entweder über DHCP oder über statische IP-Einstellungen zugewiesen werden.

Feld	Möglicher Wert	Beschreibung
	Zeichen und des Bindestrichs (-).	Eine Änderung des Onboard Administrator-DNS-Namens kann zu Unstimmigkeiten mit dem Hostnamen auf dem SSL-Zertifikat führen. Möglicherweise müssen die Zertifikatinformationen auf dem betroffenen Onboard Administrator über den Bildschirm „Certificate Administration“ (Zertifikatverwaltung) des aktiven Onboard Administrator-Moduls (Registerkarte „Certificate Administration Information“ (Zertifikatsverwaltungsinformationen) auf Seite 216) bzw. über den Bildschirm „Certificate Administration“ (Zertifikatverwaltung) des Standby-Onboard Administrator-Moduls (Registerkarte „Information“ (Informationen) auf dem Bildschirm „Standby Onboard Administrator Certificate Administration“ (Zertifikatverwaltung des Onboard Administrator-Standby-Moduls) auf Seite 232) aktualisiert werden.
MAC Address (MAC-Adresse)	Dieses Feld dient Informationszwecken und kann nicht geändert werden.	Die Onboard Administrator-MAC-Adresse.
Domain Name (Domänenname)	Dieses Feld dient Informationszwecken und kann nicht geändert werden.	Zeigt den aktuellen Domänennamen für die einzelnen Onboard Administrator-Module an.
IP Address (DNS-Adresse)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Statische IP-Adresse für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).
Subnet Mask (Subnetzmaske)	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Subnetzmaske für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).
Gateway	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Gatewayadresse für Onboard Administrator (erforderlich, wenn statische IP-Einstellungen ausgewählt sind).
IPv4 DNS 1	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IPv4-Adresse des ersten IPv4 DNS-Servers.*
IPv4 DNS 2	###.###.###.###, wobei ### einen Wert im Bereich von 0 bis 255 einnimmt	Die IPv4-Adresse des zweiten IPv4 DNS-Servers.*

* Die Reihenfolge, in der der Onboard Administrator DNS-Server verwendet, wird im Anschluss an diese Tabelle beschrieben.

Je nachdem, wie viele DNS-Server konfiguriert sind, kann Onboard Administrator bis zu sechs DNS-Server zur Suche nach einer IP-Adresse verwenden: zwei IPv4 DNS-Server (entweder statisch oder über DHCP zugewiesen, jedoch nicht beides) und vier IPv6 DNS-Server (entweder statisch oder über DHCP zugewiesen oder beides). Onboard Administrator verwendet die DNS-Server in der folgenden Reihenfolge:

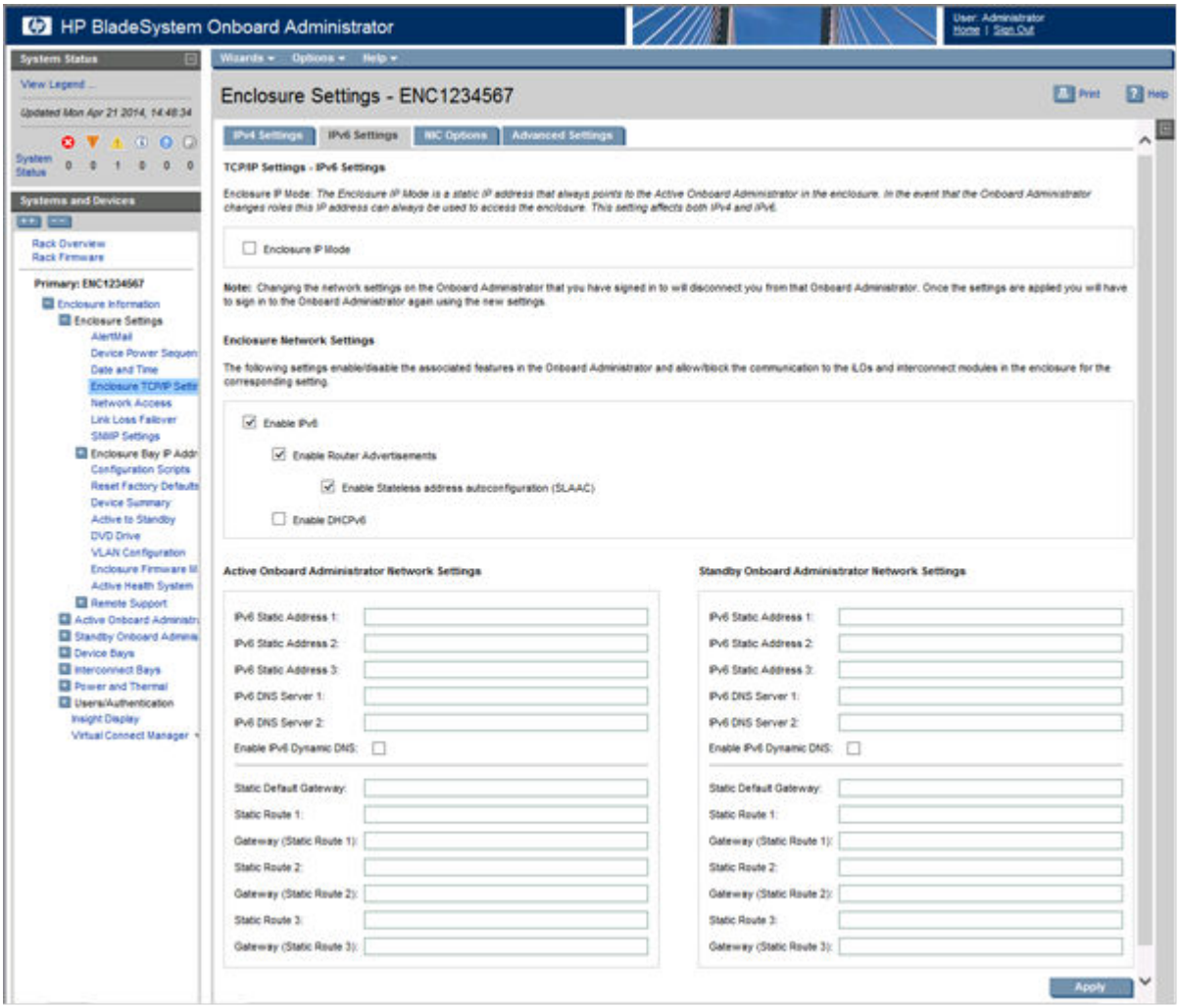
1. IPv4 DNS-Server 1 (statisch)
2. IPv6 DNS-Server 1 (statisch)

3. IPv4 DNS-Server 2 (statisch)
4. IPv6 DNS-Server 2 (statisch)
5. IPv4 DNS-Server 1 (über DHCP zugewiesen)
6. IPv6 DNS-Server 1 (über DHCP zugewiesen)
7. IPv4 DNS-Server 2 (über DHCP zugewiesen)
8. IPv6 DNS-Server 2 (über DHCP zugewiesen)

Wenn irgendwelche der DNS-Server in dieser Liste nicht konfiguriert sind, dann rücken die nachfolgenden DNS-Server in der Liste entsprechend auf. Angenommen, die über DHCP zugewiesenen IPv4 DNS-Server 1 und 2 sind nicht konfiguriert. In diesem Fall rücken dann die zwei über DHCP zugewiesenen IPv6 DNS-Server in der Liste auf Platz 5 und 6 auf. Wie bereits erwähnt, können IPv4 DNS-Server nur statisch oder über DHCP (jedoch nicht beides) zugewiesen werden. Daher kann der Onboard Administrator maximal 6 DNS-Server nutzen.

Um die neuen IPv4-Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Registerkarte „IPv6 Settings“ (IPv6-Einstellungen)



Enclosure IP Mode (Gehäuse-IP-Modus)

Wenn die Einstellung **Enclosure IP Mode** (Gehäuse-IP-Modus) aktiviert ist, wird mit ihr sichergestellt, dass alle Verwaltungsanwendungen mittels einer einzelnen statischen IP-Adresse auf das aktive Onboard Administrator-Modul des Gehäuses verweisen. Dieser Modus ist für Gehäuse mit einem aktiven und einem Onboard Administrator Standby-Modul bestimmt. Wenn das Onboard Administrator-Standby-Modul die Rolle des aktiven Onboard Administrator-Moduls übernimmt, wird dem betreffenden Onboard Administrator-Modul die IP-Adresse des vorherigen aktiven Onboard Administrator-Moduls zugewiesen. Dadurch wird sichergestellt, dass die IP-Adresse von **Enclosure IP Mode** (Gehäuse-IP-Modus) ständig auf das aktive Onboard Administrator-Modul verweist.

Für den **Enclosure IP Mode** (Gehäuse-IP-Modus) muss der aktive Onboard Administrator über eine statische IPv4- oder eine statische IPv6-Adresse verfügen (IPv6 muss aktiviert sein). Das Onboard Administrator Standby-Modul kann für DHCP oder statische IP-Einstellungen konfiguriert werden. Dieser Modus ist optional und standardmäßig deaktiviert.

Um sicherzustellen, dass die Einstellung **Enclosure IP Mode** (Gehäuse-IP-Modus) beim Entfernen eines Onboard Administrator-Moduls aus dem Gehäuse nicht geändert wird, darf das Modul nicht in der Failover-Übergangsphase (etwa sechs Minuten nach einem Failover) entfernt werden. Um nach dem Entfernen eines Moduls sicherzustellen, dass alle Einstellungen auf das Standby-Modul übertragen werden, fügen Sie ein Ersatzmodul hinzu und lassen Sie fünf Minuten lang angeschlossen. Sollten das aktive und das Standby-Onboard Administrator-Modul gleichzeitig ausgeschaltet oder aus dem Gehäuse entfernt werden, wird das Standby-Onboard Administrator-Modul auf die Standardnetzwerkeinstellungen zurückgesetzt und alle manuell konfigurierten statischen Netzwerkadressen gehen verloren.

HINWEIS: Diese Funktion ist im FIPS-Modus ON/DEBUG deaktiviert.

HINWEIS: Wenn **Enclosure IP Mode** (Gehäuse-IP-Modus) auf der Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) oder auf der Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) aktiviert wird, wird dieser Modus automatisch auf beiden Registerkarten aktiviert.

Enclosure Network Settings (Netzwerkeinstellungen des Gehäuses)

IPv6 unterstützt mehrere Adressen. Es können beliebige Kombinationen der Netzwerkeinstellungen aktiviert werden. Bei Aktivierung von IPv6, SLAAC und/oder DHCPv6 kann der Onboard Administrator von allen ausgewählten Quellen IP-Adressen beziehen. Er kann über automatisch zugewiesene IP-Adressen und vom Benutzer angegebene statische IP-Adressen verfügen. Die Einstellungen **Enable SLAAC** (SLAAC aktivieren), **Enable DHCPv6** (DHCPv6 aktivieren) und **Enable Router Advertisements** (Routerankündigungen aktivieren) werden nur wirksam, wenn IPv6 aktiviert ist.

- **Enable IPv6** (IPv6 aktivieren): Aktiviert das IPv6-Protokoll für alle Onboard Administrator-, Verbindungs- und Server-iLO-Module im Gehäuse. Sofern aktiviert, wird automatisch eine verbindungslokale Adresse konfiguriert.
- **Enable Router Advertisements** (Routerankündigungen aktivieren): Ermöglicht IPv6-Routerankündigungen vom externen Verwaltungsnetzwerk im internen Gehäuseverwaltungsnetzwerk. Wenn Sie diese Einstellung deaktivieren, blockiert Onboard Administrator IPv6-Routerankündigungen, die vom externen Verwaltungsnetzwerk gesendet werden, wodurch sie am Eintritt in das interne Verwaltungsnetzwerk des Gehäuse gehindert werden.
- **Enable SLAAC** (SLAAC aktivieren): Aktiviert Benachrichtigungen über die zustandslose automatische Konfiguration von IPv6-Adressen an alle Onboard Administrator-, Verbindungs- und Server-iLO-Module im Gehäuse. Diese Funktion wirkt sich nur auf globale IPv6-

Adressen aus. Wenn IPv6 und SLAAC beide aktiviert wird, kann der Onboard Administrator bis zu 11 SLAAC-IP-Adressen beziehen.

- **Enable DHCPv6** (DHCPv6 aktivieren): Ermöglicht dem aktiven (und, sofern aktiviert, dem Standby-) Onboard Administrator, eine DHCPv6-IP-Adresse anzufordern. Ermöglicht DHCPv6-Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk.

ACHTUNG: Wenn Sie IPv6 in einer reinen IPv6-Umgebung deaktivieren, geht die Verbindung zur Onboard Administrator-GUI und allen SSH-Sitzungen verloren. Um Ihre Verbindung wieder aufzubauen, müssen Sie die Erstkonfiguration des Gehäuses über das IPv4-Netzwerk, das Insight Display oder die serielle Schnittstelle der Onboard Administrator-Konsole durchführen. Wenn Sie IPv6, SLAAC oder DHCPv6 deaktivieren, werden alle Verbindungen, die vom deaktivierten Protokoll abhängig sind, geschlossen. Angenommen, Sie sind mit dem Onboard Administrator über dessen DHCPv6-zugewiesene Adresse verbunden. Wenn die DHCPv6-Einstellung des Gehäuses deaktiviert wird, hat dies zur Folge, dass Ihre Sitzung geschlossen wird.

HINWEIS: Damit SLAAC-Adressen erfolgreich konfiguriert werden, müssen die Einstellungen **Enable SLAAC** (SLACC aktivieren) und **Enable Router Advertisements** (Routerankündigungen aktivieren) auf dem Gehäuse aktiviert sein. Darüber hinaus muss ein IPv6-Router auf dem Gehäuse-Verwaltungsnetzwerk konfiguriert werden, um die SLAAC-Adressen über Routerankündigungen bereitzustellen. iLOs müssen zum Anfordern von SLAAC-Adressen möglicherweise separat konfiguriert werden. Die Einstellungen **Enable SLAAC** (SLAAC aktivieren), **Enable Router Advertisements** (Routerankündigungen aktivieren) und **Enable IPv6** (IPv6 aktivieren) müssen aktiviert sein, um den erforderlichen Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk zu ermöglichen.

HINWEIS: Damit DHCPv6-Adressen erfolgreich konfiguriert werden, muss die Einstellung **Enable IPv6** (IPv6 aktivieren) aktiviert sein und auf dem Verwaltungsnetzwerk muss ein DHCPv6-Server konfiguriert sein. Alle iLOs und Verbindungsmodule müssen zum Anfordern einer DHCPv6-Adresse separat konfiguriert werden. Wenn sie zum Anfordern von DHCPv6-Adressen konfiguriert sind, müssen die Einstellungen **Enable IPv6** (IPv6 aktivieren) und **Enable DHCPv6** (DHCPv6 aktivieren) aktiviert sein, um den erforderlichen Datenverkehr auf dem Gehäuse-Verwaltungsnetzwerk zu ermöglichen.

HINWEIS: Nach dem Zurücksetzen auf die Werkseinstellungen sind die IPv6-Netzwerkeinstellungen für IPv6, SLAAC, DHCPv6 und Routerankündigungen des Gehäuses standardmäßig aktiviert.

Netzwerkeinstellungen des aktiven und des Standby-Onboard Administrator-Moduls

HINWEIS: Bei einer Änderung der Netzwerkeinstellungen auf dem Onboard Administrator, bei dem Sie angemeldet sind, wird Ihre Verbindung mit dem Onboard Administrator möglicherweise getrennt. In diesem Fall müssen Sie sich nach dem Anwenden der Einstellungen wieder bei dem Onboard Administrator anmelden.

Feld	Möglicher Wert	Beschreibung
IPv6 Static Address 1 (Statische IPv6 Adresse 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 1 des externen Onboard Administrator-NIC.

Feld	Möglicher Wert	Beschreibung
IPv6 Static Address 2 (Statische IPv6 Adresse 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 2 des externen Onboard Administrator-NIC.
IPv6 Static Address 3 (Statische IPv6 Adresse 3)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF und das Präfix /### im Bereich von 1 bis 128 liegt.[1,2]	IPv6-Adresse 3 des externen Onboard Administrator-NIC.
IPv6 DNS Server 1 (IPv6 DNS-Server 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt. Das Präfix ist optional.[1]	Die IPv6-Adresse des ersten statischen IPv6 DNS-Servers.[3]
IPv6 DNS Server 2 (IPv6 DNS-Server 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt. Das Präfix ist optional.[1]	Die IPv6-Adresse des zweiten statischen IPv6 DNS-Servers.[3]
Enable IPv6 Dynamic DNS (Dynamisches IPv6-DNS aktivieren)	Aktiviert (Kontrollkästchen ausgewählt) oder deaktiviert (Kontrollkästchen nicht ausgewählt).	Ermöglicht Ihnen, für den Onboard Administrator einen Hostnamen zu verwenden, der auch dann noch beibehalten wird, wenn sich die dynamisch zugewiesene IP-Adresse ändern sollte. Der Hostname wird bei einem DNS-Server registriert. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Datensätzen für IP-Adressen.[4] Wenn „Dynamic DNS“ (Dynamisches DNS) auf Onboard Administrator deaktiviert wird, werden die Onboard Administrator-Aktualisierungen am DNS-Server gestoppt. Es ist jedoch zu beachten, dass bei einigen DHCP-Servern eine Regelung die direkte Aktualisierung von DNS-Servern ermöglicht. Um dynamische DNS-Aktualisierungen vollständig zu deaktivieren, müssen Sie „Dynamic DNS“ (Dynamisches DNS) sowohl auf dem Onboard Administrator als auch auf dem DHCP-Server deaktivieren.
Static Default Gateway (Statisches Standard-Gateway)	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Es wird vorausgesetzt, dass das Gateway vom Onboard Administrator-Netzwerk aus erreichbar ist.[1]	Die statische IPv6-Adresse des Standard-Gateways. Diese Einstellung ist in einer IPv6-Netzwerkumgebung erforderlich, die konfigurationsgemäß vollständig statisch ist. Onboard Administrator kann die IPv6-Gatewaykonfiguration direkt über diese Einstellung akzeptieren und, sofern Routerankündigungen konfiguriert sind, über Routerankündigungen von IPv6-Routern im Verwaltungsnetzwerk. Wenn die IPv6-Gatewaykonfiguration über Routerankündigungen bereitgestellt wird, wird die statische IPv6-Gateway-Einstellung durch die Gatewaykonfiguration der Routerankündigungen übersteuert. Das derzeit von dem Onboard Administrator verwendete IPv6-Gateway wird auf dem Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) (Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator auf Seite 212) des aktiven Onboard Administrator und auf dem Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen)

Feld	Möglicher Wert	Beschreibung
		des Standby-Onboard Administrator im Feld „Current Default Gateway“ (Aktuelles Standard-Gateway) angezeigt.
Static Route 1 (Statischer Verbindungsweg 1)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration).[5] Der statische Verbindungsweg definiert einen expliziten Pfad, den der Onboard Administrator verwendet, um über ein Gateway ein externes Netzwerk zu erreichen. In einer statischen Netzwerkkonfiguration ist es aufgrund des statischen Verbindungswegs nicht notwendig, einen Router zum Senden von Verbindungsweginformationen über Routerankündigungen zu konfigurieren. Wenn in einem Netzwerk mit aktiven Routerankündigungen das Standard-Gateway bereits konfiguriert ist, teilt der Router allen Knoten die verfügbaren statischen Verbindungswege mit. In diesem Fall ist eine manuelle Konfiguration der statischen Verbindungswege nicht erforderlich. Wenn Sie den statischen Verbindungsweg 1 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 1) angeben.
Gateway (Static Route 1) (Gateway (Statischer Verbindungsweg 1))	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen Netzwerk aus erreichbar sein.[1]	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 1 definierten Pfades. Sie müssen auch den statischen Verbindungsweg 1 angeben.
Static Route 2 (Statischer Verbindungsweg 2)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen zweiten statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration). Wenn Sie den statischen Verbindungsweg 2 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 2) angeben.
Gateway (Static Route 2) (Gateway (Statischer Verbindungsweg 2))	####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen Netzwerk aus erreichbar sein.[1]	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 2 definierten Pfades. Sie müssen auch den statischen Verbindungsweg 2 angeben.
Static Route 3 (Statischer Verbindungsweg 3)	####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt und das Präfix /### im Bereich von 1 bis 128 liegt.[1]	Fügt der Routingtabelle von Onboard Administrator einen dritten statischen IPv6-Verbindungsweg hinzu (manuelle Konfiguration). Wenn Sie den statischen Verbindungsweg 3 angeben, müssen Sie auch das zugehörige Gateway (Statischer Verbindungsweg 3) angeben.
Gateway (Static Route 3) (Gateway (Statischer Verbindungsweg 3))	####:####:####:####:####:####:####:####, wobei #### im Bereich von	Die IPv6-Adresse des Gateways unter Verwendung des durch den statischen Verbindungsweg 3 definierten Pfades.

Feld	Möglicher Wert	Beschreibung
	0 bis FFFF liegt. Geben Sie kein Präfix an. Das Gateway muss sowohl vom Onboard Administrator-Netzwerk als auch vom externen Netzwerk aus erreichbar sein.[1]	Sie müssen auch den statischen Verbindungsweg 3 angeben.

[1] Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
[2] Der Onboard Administrator akzeptiert als statische IPv6-Adresse keine verbindungslokale Adresse.
[3] Die Reihenfolge, in der Onboard Administrator DNS-Server verwendet, wird im Anschluss an diese Tabelle beschrieben.
[4] Für „IPv6 Dynamic DNS“ (Dynamischer IPv6-DNS) muss auf dem Onboard Administrator ein gültiger DNS-Server (entweder IPv4 oder IPv6) konfiguriert sein.
[5] **Achtung**: Das Hinzufügen oder Entfernen eines statischen Verbindungsweges kann zum Verlust der Konnektivität von Clients führen, die auf Onboard Administrator zugreifen.

Je nachdem, wie viele DNS-Server konfiguriert sind, kann Onboard Administrator bis zu sechs DNS-Server zur Suche nach einer IP-Adresse verwenden: zwei IPv4 DNS-Server (entweder statisch oder über DHCP zugewiesen, jedoch nicht beides) und vier IPv6 DNS-Server (entweder statisch oder über DHCP zugewiesen oder beides). Onboard Administrator verwendet die DNS-Server in der folgenden Reihenfolge:

1. IPv4 DNS-Server 1 (statisch)
2. IPv6 DNS-Server 1 (statisch)
3. IPv4 DNS-Server 2 (statisch)
4. IPv6 DNS-Server 2 (statisch)
5. IPv4 DNS-Server 1 (über DHCP zugewiesen)
6. IPv6 DNS-Server 1 (über DHCP zugewiesen)
7. IPv4 DNS-Server 2 (über DHCP zugewiesen)
8. IPv6 DNS-Server 2 (über DHCP zugewiesen)

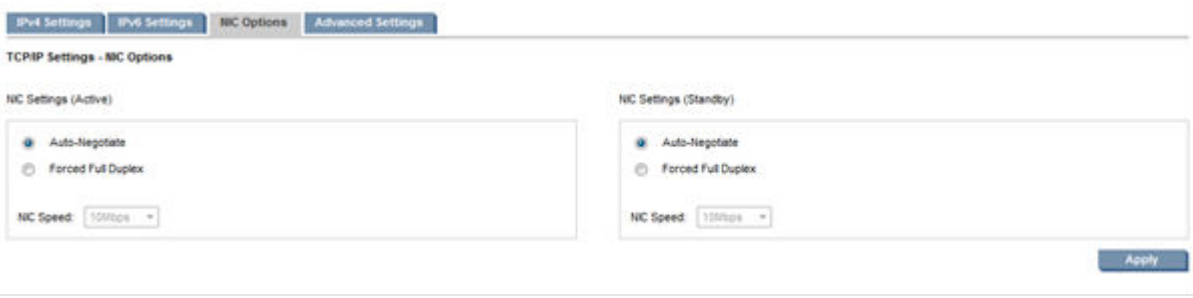
Wenn irgendwelche der DNS-Server in dieser Liste nicht konfiguriert sind, dann rücken die nachfolgenden DNS-Server in der Liste entsprechend auf. Angenommen, die über DHCP zugewiesenen IPv4 DNS-Server 1 und 2 sind nicht konfiguriert. In diesem Fall rücken dann die zwei über DHCP zugewiesenen IPv6 DNS-Server in der Liste auf Platz 5 und 6 auf. Wie bereits erwähnt, können IPv4 DNS-Server nur statisch oder über DHCP (jedoch nicht beides) zugewiesen werden. Daher kann der Onboard Administrator maximal 6 DNS-Server nutzen.

Um die neuen IPv6-Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

⚠ **ACHTUNG:** Bestimmte Browser wie z. B. Mozilla Firefox und Google Chrome, besitzen möglicherweise ein Kontrollkästchen für solche Popup-Dialogfelder, das aktiviert werden kann, um zukünftige Dialogfelder auf der Seite zu verhindern. Aktivieren Sie das Kontrollkästchen in keinem dieser Dialogfelder. Andernfalls bleiben die Dialogfelder ausgeblendet, bis die Anwendung geschlossen und in einem Fenster auf einer neuen Registerkarte wieder geladen wird.

HINWEIS: Wenn Sie die Einstellungen ändern und auf **Apply** (Übernehmen) klicken, werden Sie in einer Popup-Meldung gewarnt, dass bei einer Änderung Ihrer Netzwerkeinstellungen möglicherweise Ihre Verbindung zum Onboard Administrator getrennt wird. Wenn die Änderungen beim Klicken auf **OK** bestimmte Protokolle deaktivieren, werden Sie in einer weiteren Popup-Meldung davor gewarnt, dass alle Verbindungen, die diese Protokolle verwenden, geschlossen werden und Sie möglicherweise Ihre Sitzung verlieren. Sie werden aufgefordert zu bestätigen, ob Sie diese Aktion durchführen möchten (klicken Sie auf **OK** oder **Cancel** (Abbrechen)).

Registerkarte „NIC Options“ (NIC-Optionen)



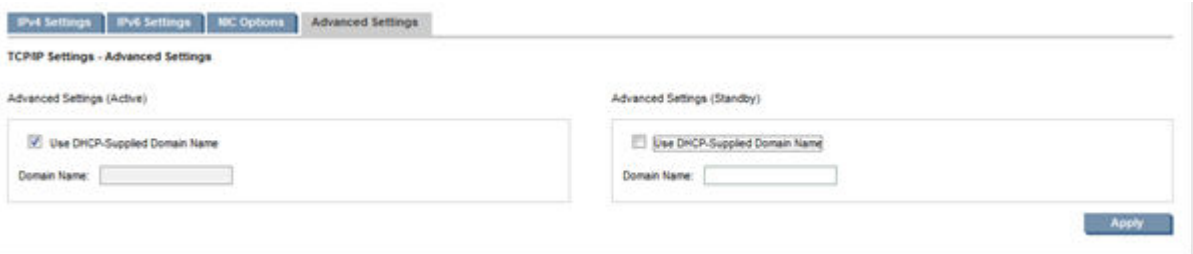
TCP/IP Settings - NIC Options (TCP/IP-Einstellungen - NIC-Optionen)

NIC settings (NIC-Einstellungen)

- **Auto-Negotiate** (Automatische Aushandlung) – Konfiguriert automatisch den besten Link. Dies ist die Standardeinstellung. Diese Option unterstützt eine NIC-Geschwindigkeit von 10 MB/s, 100 MB/s oder 1000 MB/s. 1000 MB/s sind nur bei Auswahl der Option „Auto-Negotiate“ (Automatische Aushandlung) verfügbar.
- **Forced Full Duplex** (Erzwungener Vollduplex) – Bei dieser Einstellung können Sie manuell festlegen, welche Einstellungen der externe NIC beim Aufbau eine Verbindung verwendet. Onboard Administrator überprüft nicht, ob die erzwungenen Ethernet-Einstellungen im Netzwerk gültig sind. Es kann daher ein Kommunikationsverlust auftreten, wenn falsche oder inkompatible Einstellungen verwendet werden. Erzwungene Einstellungen werden 3 Sekunden nach dem Aktivieren oder Deaktivieren der Einstellungen wirksam. Die erzwungene Option unterstützt nur die NIC-Geschwindigkeiten 10 MB/s und 100 MB/s.
- **NIC Speed** (NIC-Geschwindigkeit) – Wählt als NIC-Geschwindigkeit 10 MB/s oder 100 MB/s.

Um die neuen Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Registerkarte „Advanced Settings“ (Erweiterte Einstellungen)



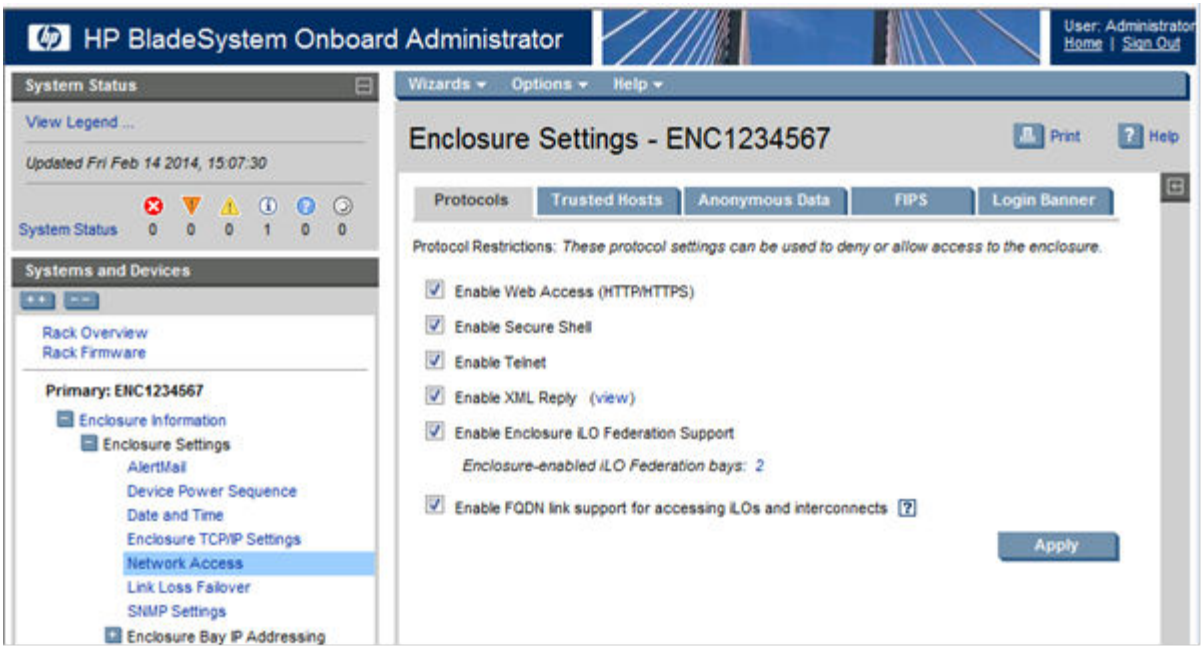
Dieser Bildschirm zeigt die aktuellen Gehäuse-TCP/IP-Einstellungen („Advanced Settings“ (Erweiterte Einstellungen)) für das aktive Onboard Administrator-Modul an. Auf der Registerkarte „Advanced Settings“ (Erweiterte Einstellungen) können Sie die Option **DHCP-Supplied Domain Name** (Über DHCP bereitgestellter Domänenname) aktivieren oder deaktivieren. Um die Eingabe von durch den Benutzer bereitgestellten Domänennamen für „Active“ (Aktiv) und „Standby“ (Standby) zu ermöglichen, ist die Option **DHCP-Supplied Domain Name** (Über DHCP bereitgestellter

Domänenname) deaktiviert. Zum Aktivieren oder Deaktivieren der Option **DHCP-Supplied Domain Name** (Über DHCP bereitgestellter Domänenname) oder zum Festlegen von vom Benutzer bereitgestellten Domänennamen muss „Dynamic DNS“ (Dynamischer DNS) aktiviert sein. Verwenden Sie zum Aktivieren von „Dynamic DNS“ (Dynamisches DNS) die Registerkarte „IPv4 Settings“ (IPv4-Einstellungen, Registerkarte „IPv4-Einstellungen“ auf Seite 126) oder die Registerkarte „IPv6 Settings“ (IPv6-Einstellungen, Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf Seite 129).

Um den über DHCP bereitgestellten Domänennamen manuell zu überschreiben, entfernen Sie die Markierung des Kontrollkästchens **Use DHCP-Supplied Domain Name** (Über DHCP bereitgestellten Domänennamen verwenden), und geben Sie dann den Domänennamen ein. Klicken Sie auf **Apply** (Übernehmen).

HINWEIS: Wenn das Kontrollkästchen **Use DHCP-Supplied Domain Name** (Über DHCP bereitgestellten Domänennamen verwenden) markiert ist, können Sie das Feld für den Domänennamen nicht bearbeiten.

Network Access (Netzwerkzugriff)



Mittels dieser Einstellungen kann ein Administrator Einstellungen bezüglich des Netzwerkzugriffs auf den Onboard Administrator konfigurieren. Diese Einstellungen sind gehäusespezifisch und wirken sich nicht auf die Netzwerkkonfigurationen für Server Blades aus.

Registerkarte „Protocols“ (Protokolle)

Es stehen die folgenden Protokolleinstellungen zur Auswahl, mit denen der Zugriff auf Onboard Administrator gestattet oder eingeschränkt werden kann.

- **Enable Web Access (HTTP/HTTPS)** (Webzugriff aktivieren (HTTP/HTTPS)) – Dieses Kontrollkästchen ist standardmäßig markiert. Wenn Sie seine Auswahl aufheben, wird der HTTP/HTTPS-Zugriff auf Onboard Administrator deaktiviert. Port 80 wird für HTTP und Port 443 wird für HTTPS verwendet.

ACHTUNG: Durch das Deaktivieren des Webzugriffs (HTTP/HTTPS) werden alle Benutzer, die über HTTP/HTTPS mit Onboard Administrator verbunden sind – einschließlich Administrator – getrennt.

- **Enable Secure Shell** (Secure Shell aktivieren) – Dieses Kontrollkästchen ist standardmäßig markiert. Wenn Sie seine Auswahl aufheben, werden Secure Shell-Verbindungen zu Onboard Administrator deaktiviert. SSH ist deaktiviert, wenn „Two-Factor Authentication“ (2-Faktor-Authentifizierung) aktiviert ist. Durch Deaktivieren der 2-Faktor-Authentifizierung wird SSH nicht automatisch wieder aktiviert. Um SSH wieder zu aktivieren, müssen Sie das Kontrollkästchen markieren und danach auf **Apply** (Übernehmen) klicken. Port 22 wird für SSH verwendet.
- **Enable Telnet** (Telnet aktivieren): Dieses Kontrollkästchen ist standardmäßig markiert. Wenn Sie dieses Kontrollkästchen auswählen, werden Telnet-Verbindungen zu Onboard Administrator aktiviert. Telnet ist deaktiviert, wenn „Two-Factor Authentication“ (2-Faktor-Authentifizierung) aktiviert ist. Durch Deaktivieren der 2-Faktor-Authentifizierung wird Telnet nicht automatisch wieder aktiviert. Um Telnet wieder zu aktivieren, müssen Sie das Kontrollkästchen markieren und danach auf **Apply** (Übernehmen) klicken. Port 23 wird für Telnet verwendet.

HINWEIS: Wenn Onboard Administrator im FIPS-Modus ON/DEBUG betrieben wird, kann das Telnet-Protokoll nicht verwendet werden.

HINWEIS: Telnet ist nach Zurücksetzen auf die Werkseinstellungen oder bei Aktivieren von „Two-Factor Authentication“ (2-Faktor-Authentifizierung) deaktiviert.

- **Enable XML Reply** (XML-Antwort aktivieren) – Dieses Kontrollkästchen ist standardmäßig markiert. Wenn dieses Kontrollkästchen aktiviert ist, können XML-Daten von Onboard Administrator und anderen HP Verwaltungsprogrammen wie HP Systems Insight Manager gemeinsam genutzt werden. Um anzuzeigen, welche Daten von Onboard Administrator gemeinsam mit anderen Programmen genutzt werden, wenn dieses Protokoll aktiviert ist, klicken Sie auf **View** (Anzeigen).
- **Enable Enclosure iLO Federation Support** (Unterstützung für Gehäuse-iLO-Verbund aktivieren): Dieses Kontrollkästchen ist standardmäßig aktiviert. Dieses Kontrollkästchen aktiviert die Onboard Administrator-Unterstützung der Peer-to-Peer-Netzwerkkommunikation, die für einen iLO-Verbund entsprechend fähiger iLOs innerhalb des Gehäuses benötigt wird. Wenn ein iLO-Verbund für das Gehäuse unterstützt wird, zeigt der aktive Onboard Administrator die Geräteeinschubsnummer eines jeden Einschubs an, für den die Peer-to-Peer-Netzwerkkommunikation aktiviert wird, die für den iLO-Verbund erforderlich ist.

HINWEIS: **Enable Enclosure iLO Federation Support** (Unterstützung für Gehäuse-iLO-Verbund aktivieren) aktiviert die Onboard Administrator-Unterstützung zur Ermöglichung der Peer-to-Peer-Netzwerkkommunikation, die für den iLO-Verbund zwischen iLOs innerhalb des Gehäuses erforderlich ist. Um den iLO-Verbund vollständig zu aktivieren, muss jedes iLO-Modul über die entsprechende Firmware verfügen und zur Teilnahme am iLO-Verbund konfiguriert sein. Weitere Informationen enthält das *HP iLO 4 Benutzerhandbuch* auf der HP Website (http://www.hp.com/go/ilo/docs).

- **Enable FQDN link support for accessing iLOs and interconnects** (FQDN-Link-Unterstützung für den Zugriff auf iLOs und Verbindungsmodule aktivieren): Dieses Kontrollkästchen ist standardmäßig nicht aktiviert. Bei Aktivierung dieses Kontrollkästchens zeigt Onboard Administrator zusätzlich zu den üblichen IP-basierten Internet-Adressen-Links für den Zugriff auf ein iLO- oder Verbindungsmodul über die Onboard Administrator-GUI einen FQDN-basierten Internet-Adressen-Link an. Onboard Administrator ermöglicht das Abfragen eines DNS-Servers, der einen Reverse-Lookup-Vorgang für den FQDN des Geräts durchführt und und die FQDN-basierte Internetadresse erstellt (im Format Hostname.Domänenname.com). Auf dem Onboard Administrator muss ein IPv4-DNS-Server konfiguriert werden, und die Geräte, auf die

zugegriffen werden soll, müssen bei dem DNS-Namensserver für Reverse-Lookup registriert werden. Auf dem Onboard Administrator muss eine DNS-IP-Adresse konfiguriert werden (über die Registerkarte „TCP/IP IPv4 Settings“ (TCP/IP-IPv4-Einstellungen) (Registerkarte „IPv4-Einstellungen“ auf Seite 126)).

Wenn die FQDN-Einstellung aktiviert ist, werden die Listen der URL-Links für alle entsprechenden Geräte (iLOs und Verbindungsmodule) automatisch aktualisiert und mit den entsprechenden FQDNs aktualisiert. Wenn die FQDN-Einstellung deaktiviert ist, werden die FQDN-Links aller Gehäuse-Geräte vom Onboard Administrator entfernt und daher nicht angezeigt.

FQDN-Link-Unterstützung ist in IPv6-basierten Remote-Zugriffs-Umgebungen nützlich, die von einem IPv4-basierten Gehäuse-Verwaltungsnetzwerk mit IPv4-DNS abhängig sind. Sie ist nicht für reine IPv6-Umgebungen mit IPv6-DNS vorgesehen.

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Registerkarte „Trusted Hosts“ (Vertrauenswürdige Hosts)

Vertrauenswürdige Hosts

Mit der Funktion „Trusted Hosts“ (Vertrauenswürdige Hosts) können Sie den Zugriff auf Onboard Administrator einschränken.

Diese Unterkategorie enthält ein Dialogfeld, ein Eingabefeld sowie ein Anzeigefeld, in dem bei Aktivierung die vertrauenswürdigen IP-Adressen aufgeführt sind.

Das Kontrollkästchen **Enable IP address access restriction** (Zugriffsbeschränkung für IP-Adressen aktivieren) ist standardmäßig nicht aktiviert. Wenn dieses Kontrollkästchen aktiviert ist, wird nur den als „Trusted Addresses“ (Vertrauenswürdige Adressen) aufgeführten IP-Adressen eine Verbindung mit Onboard Administrator gestattet.

⚠ **ACHTUNG:** Wenn Sie die Zugriffsbeschränkung für IP-Adressen aktivieren, ohne vorher die IPAdresse des Benutzers in die Liste der vertrauenswürdigen Adressen einzutragen, wird der Benutzer von Onboard Administrator getrennt.

⚠ **ACHTUNG:** Wenn die Funktion „Trusted Hosts“ (Vertrauenswürdige Hosts) in einer Umgebung verwendet wird, in der mehrere Gehäuse über Verbindungskabel miteinander verbunden sind, ist sicherzustellen, dass alle verbundenen Gehäuse über die gleichen Einstellungen für „Trusted Hosts“ (Vertrauenswürdige Hosts) verfügen. Miteinander verbundene Gehäuse mit verschiedenen Einstellungen für „Trusted Hosts“ (Vertrauenswürdige Hosts) lassen möglicherweise zu, dass ein Benutzer der grafischen Weboberfläche über einen vertrauenswürdigen Client auf ein geschütztes Gehäuse zugreift.

⚠ **ACHTUNG:** RFC 4941 beschreibt eine IPv6-SLAAC-Erweiterung, die über sich mit der Zeit ändernden Schnittstellenkennungen das Erstellen globaler temporärer IPv6-Adressen ermöglicht. Wenn ein Betriebssystem, das RFC 4941 unterstützt, neu gestartet wird oder wenn die aktuelle Adresse abläuft, wird eine neue temporäre IPv6-Adresse erstellt. Windows 7 ist ein Beispiel solch ein Betriebssystem, das RFC 4941 unterstützt.

Wenn Sie bei aktiviertem vertrauenswürdigem Host über einen Client auf einem Betriebssystem mit RFC 4941-Unterstützung auf den Onboard Administrator zugreifen, kann ein Neustart des Client-Betriebssystems dazu führen, dass die Verbindung zum Onboard Administrator nicht mehr hergestellt werden kann. Die Verbindung schlägt fehl, da die neue temporäre IPv6-Adresse des Clients nicht mit der für den Client in der Liste „Trusted Addresses“ (Vertrauenswürdige Adressen) konfigurierten IPv6-Adresse übereinstimmt. Um dieses Problem zu vermeiden, deaktivieren Sie entweder das Erstellen globaler temporärer IPv6-Adressen im Betriebssystem oder konfigurieren Sie die IP-Adresse des vertrauenswürdigen Hosts mit der IPv6-Adresse des neu erstellten Clients neu.

Im Feld „Trusted Addresses“ (Vertrauenswürdige Adressen) werden die IP-Adressen sämtlicher Hosts eingegeben, die als vertrauenswürdig eingestuft sind und über die Protokolle, die in der Unterkategorie „Protocol Restrictions“ (Protokollbeschränkungen) festgelegt wurden, eine Remote-Verbindung zu Onboard Administrator herstellen können. Dieses Feld lässt nur die Eingabe von IP-Adressen zu. Geben Sie bei der Angabe der IPv6-Adresse keine Präfixlänge an.

Unterhalb des Feldes „Trusted Addresses“ (Vertrauenswürdige Adressen) befindet sich das Listenfeld mit allen vertrauenswürdigen IP-Adressen, falls vertrauenswürdige IP-Adressen konfiguriert sind.

Zum Hinzufügen eines vertrauenswürdigen Hosts geben Sie die zugehörige IP-Adresse im Feld „Trusted Addresses“ (Vertrauenswürdige Adressen) ein und klicken auf **Add** (Hinzufügen). Sie können maximal fünf vertrauenswürdige Adressen eingeben.

Zum Entfernen eines vertrauenswürdigen Hosts markieren Sie die zugehörige IP-Adresse in der Liste „Trusted Addresses“ (Vertrauenswürdige Adressen) und klicken auf **Remove** (Entfernen).

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

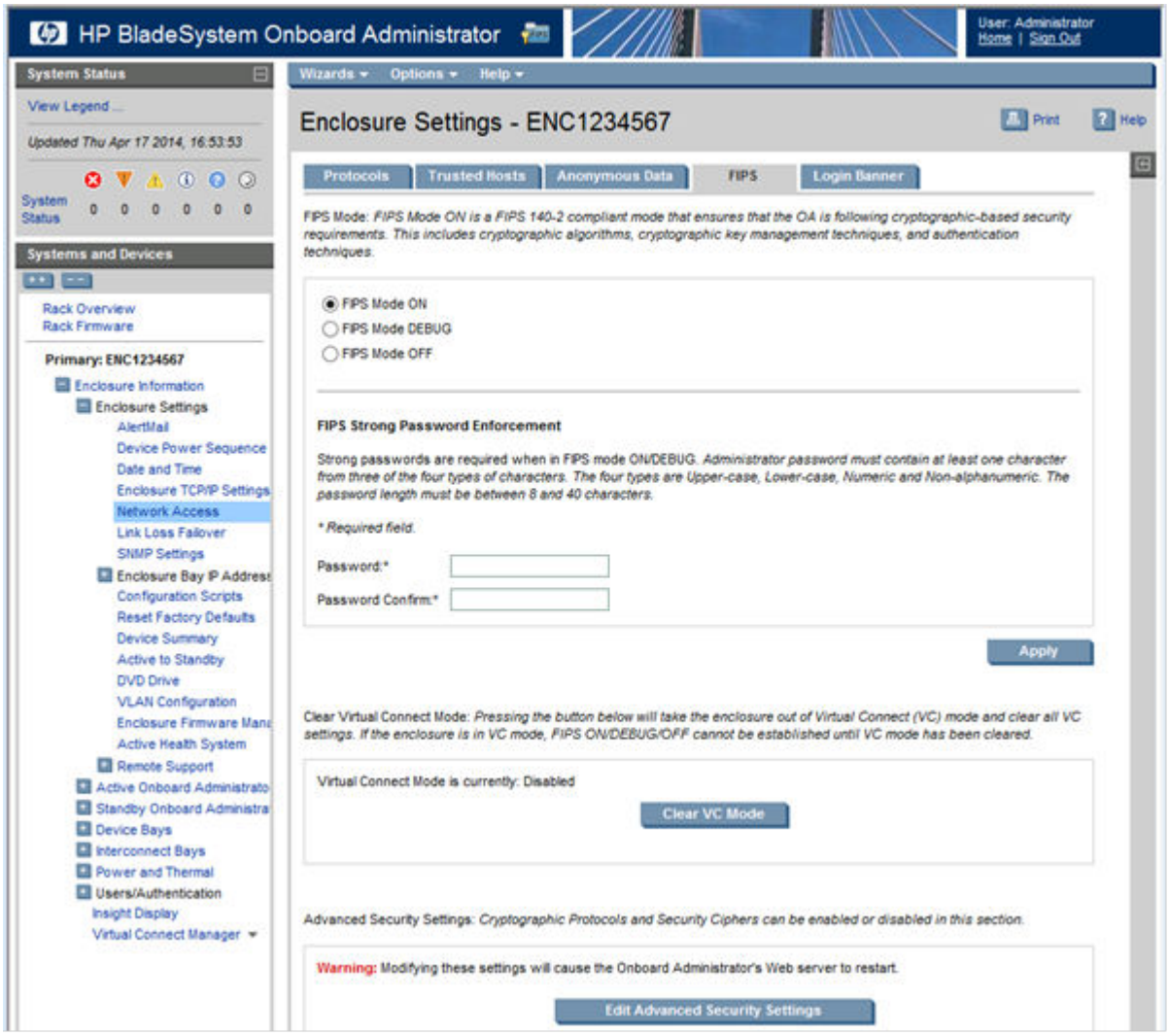
Registerkarte „Anonymous Data“ (Anonyme Daten)

Enable Extended Data on GUI Login Page (Erweiterte Daten auf GUI-Anmeldeseite aktivieren): Dieses Kontrollkästchen ist standardmäßig aktiviert. Durch Deaktivieren dieses Kontrollkästchens wird die „+“-Funktionalität in der Topologieansicht auf der Anmeldeseite dieses Gehäuses deaktiviert. Außerdem wird der Zustand von Onboard Administrator auf der Anmeldeseite als `N/A` (Nicht zutreffend) angegeben.

Wenn die Seite für erweiterte Daten auf der GUI-Anmeldeseite deaktiviert ist, können authentifizierte Benutzer keine weiteren Informationen anzeigen. Um zu verhindern, dass zusätzliche Informationen für die einzelnen verbundenen Gehäuse angezeigt werden, müssen Sie dieses Kontrollkästchen für jedes Gehäuse deaktivieren.

Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Registerkarte „FIPS“


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend
Updated Thu Apr 17 2014, 16:53:53
System Status
0 0 0 0 0 0
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Address
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Mani
Active Health System
Remote Support
Active Onboard Administrato
Standby Onboard Administra
Device Bays
Interconnect Bays
Power and Thermal
Users/Authentication
Insight Display
Virtual Connect Manager
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Protocols
Trusted Hosts
Anonymous Data
FIPS
Login Banner
FIPS Mode: FIPS Mode ON is a FIPS 140-2 compliant mode that ensures that the OA is following cryptographic-based security requirements. This includes cryptographic algorithms, cryptographic key management techniques, and authentication techniques.
FIPS Mode ON
FIPS Mode DEBUG
FIPS Mode OFF
FIPS Strong Password Enforcement
Strong passwords are required when in FIPS mode ON/DEBUG. Administrator password must contain at least one character from three of the four types of characters. The four types are Upper-case, Lower-case, Numeric and Non-alphanumeric. The password length must be between 8 and 40 characters.
* Required field.
Password:*
Password Confirm:*
Apply
Clear Virtual Connect Mode: Pressing the button below will take the enclosure out of Virtual Connect (VC) mode and clear all VC settings. If the enclosure is in VC mode, FIPS ON/DEBUG/OFF cannot be established until VC mode has been cleared.
Virtual Connect Mode is currently: Disabled
Clear VC Mode
Advanced Security Settings: Cryptographic Protocols and Security Ciphers can be enabled or disabled in this section.
Warning: Modifying these settings will cause the Onboard Administrator's Web server to restart.
Edit Advanced Security Settings

FIPS-Modus

HINWEIS: Änderungen des FIPS-Modus in ON/DEBUG oder OFF werden nur wirksam, wenn der VC-Modus deaktiviert ist.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

- **FIPS Mode OFF** (FIPS-Modus AUS): Ermöglicht die Verwendung von nicht FIPS-140-2-genehmigten Algorithmen.
- **FIPS Mode ON** (FIPS-Modus EIN): Erzwingt die Verwendung von Onboard Administrator in einem FIPS 140-2-genehmigten Modus. Diese Einstellung unterstützt die Verwendung von genehmigten kryptographischen Protokollen und Chiffren.
- **FIPS Mode DEBUG** (FIPS-Modus DEBUG): Stellt den Onboard Administrator auf eine Umgebung ähnlich dem FIPS-Modus ON ein, jedoch mit optionaler Debug-Unterstützung von HP. Der FIPS-Modus DEBUG besitzt die Funktionalität des FIPS-Modus ON, wird aufgrund der Debug-Option jedoch nicht als FIPS-konform angesehen.

Nach Vornahme aller Änderungen wird Onboard Administrator neu gestartet.

HINWEIS: Wenn dieser Vorgang ausgeführt wird, gehen alle bestehenden Einstellungen verloren. Bei einer Änderung der FIPS MODE-Einstellung wird der Vorgang „Restore to Factory Default“ (Auf Werkseinstellungen zurücksetzen) durchgeführt.

HINWEIS: Sorgen Sie im FIPS-Modus ON/DEBUG dafür, dass ein starkes Kennwort festgelegt wurde.

Symbole des Status des FIPS-Modus

Wenn der FIPS-Modus ON oder DEBUG aktiviert ist, wird der aktuelle Status des FIPS-Modus durch ein Symbol in der Onboard Administrator-Kopfleiste auf den GUI-Bildschirmen angezeigt. Er wird auch auf der Onboard Administrator-Anmeldeseite in der Spalte „Connection“ (Verbindung) der Gehäusetabelle angezeigt. Die Symbole des Status werden in der folgenden Tabelle beschrieben:

Symbol des FIPS-Modus	Beschreibung
	Der FIPS-Modus ist aktiviert (ON).
	Für den FIPS-Modus ON sind eine oder mehrere Warnungen vorhanden. Bewegen Sie den Mauszeiger über das Symbol, um zu bestimmen, um welche Art von Warnung es sich handelt.
	Der FIPS-Modus DEBUG ist aktiviert.
	Für den FIPS-Modus DEBUG sind eine oder mehrere Warnungen vorhanden. Bewegen Sie den Mauszeiger über das Symbol, um zu bestimmen, um welche Art von Warnung es sich handelt.

Erzwingung von strengen FIPS-Kennwörtern

Wenn zwischen den verfügbaren FIPS-Modi gewechselt wird, werden starke Kennwörter aktiviert, werden als Mindestkennwortlänge acht Zeichen festgelegt und wird ein neues Kennwort für das Administratorkonto angefordert. Außerdem werden beim Wechsel zu FIPS-Modus ON oder FIPS-Modus DEBUG der Gehäuse-IP-Modus und Telnet sowie SNMPv1- und SNMPv2-Protokolle deaktiviert, und SNMPv3 ist verfügbar.

HINWEIS: Beim Aufrufen und Beenden des FIPS-Modus werden die Werkseinstellungen wiederhergestellt und wird das Insight Display (LCD) gesperrt. Wenn der Onboard Administrator zuvor mit einer statischen IP-Adresse konfiguriert war, wird standardmäßig eine DHCP-Adresse eingestellt, bis er mit einer statischen IP-Adresse neu konfiguriert wird. Für eine Wiederherstellung ist Zugriff auf die serielle Onboard Administrator-Konsole zum Ausführen des Befehls `SHOW OA NETWORK` erforderlich, mit dem die neue Onboard Administrator-IP-Adresse ermittelt wird.

Der Begriff „FIPS-Modus“ wird in diesem Dokument und im Produkt zur Beschreibung der Funktion und nicht ihres Validierungsstatus verwendet. Da der FIPS-Prüfvorgang aufwändig ist, werden nicht alle Versionen geprüft. Informationen zum aktuellen FIPS-Status dieser oder einer beliebigen anderen Firmwareversion finden Sie in den folgenden Dokumenten:

- Cryptographic Module Validation Program FIPS 140-1 and FIPS 140-2 Modules In Process List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf)
- FIPS 140-1 and FIPS 140-2 Vendor List (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)

Löschen des VC-Modus

Bei Löschen des VC-Modus werden alle VC-Einstellungen vom Gehäuse gelöscht. Schalten Sie vor dem Löschen des VC-Modus alle VC-konfigurierten Server aus. Server, die nicht ausgeschaltet werden, behalten möglicherweise ihre VC-Einstellungen bei, bis sie neu gestartet werden. Der VC-Modus muss gelöscht werden, bevor die Einstellung des FIPS-Modus von OFF in ON/DEBUG oder umgekehrt geändert wird.

So löschen Sie den VC-Modus:

1. Klicken Sie auf **Clear VC Mode** (VC-Modus löschen). Es wird ein Bestätigungsbildschirm mit folgender Meldung angezeigt: `All servers should be powered off and not configured by Virtual Connect prior to clearing VC mode. Are you sure that you wish to clear VC mode?`
2. Klicken Sie auf **OK**.

Erweiterte Sicherheitseinstellungen

Die FIPS-Sicherheitsanforderungen können sich für eine bestimmte Umgebung oder mit zunehmender Anfälligkeit bestehender Chiffren für Attacken ändern. Im FIPS-Modus ON/DEBUG kann der OA-Administrator die Sicherheitseinstellungen durch Aktivieren oder Deaktivieren ausgewählter kryptographischer TLS-Protokolle und Chiffren anpassen, die Onboard Administrator zum Aushandeln sicherer Verbindungen verwenden kann. Unterstützte Protokolle und Chiffren werden unter „Kryptographische Sicherheitsfunktionen und Standardeinstellungen“ (Kryptographische Sicherheitsfunktionen und Standardeinstellungen auf Seite 18) aufgelistet.

ACHTUNG: Wenn eine oder mehrere Chiffren deaktiviert werden, kann dies je nach der Reihenfolge und Liste der vom Client unterstützten Chiffren zur Folge haben, dass einige Clients ihre Konnektivität zur Onboard Administrator-GUI verlieren.

HINWEIS: Nachdem die Einstellungen übernommen wurden, wird der Onboard Administrator-Webdienst neu gestartet.

So ändern Sie die erweiterten Sicherheitseinstellungen:

1. Zeigen Sie durch Klicken auf die Schaltfläche **Edit Advanced Security Settings** (Erweiterte Sicherheitseinstellungen bearbeiten), die nur im FIPS-Modus ON/DEBUG angezeigt wird, die Liste der unterstützten kryptographischen Protokolle und Chiffren an.
2. Um ein Protokoll oder eine Chiffre zu aktivieren oder zu deaktivieren, aktivieren bzw. deaktivieren Sie das zugehörige Kontrollkästchen. Es können nicht alle Protokolle oder alle Chiffren deaktiviert werden. Mindestens ein Protokoll und eine Chiffre müssen immer aktiviert sein.
3. Klicken Sie auf **Apply** (Übernehmen).

Registerkarte „Login Banner“ (Anmelde-Banner)

Zum Aktivieren der Option „Login Banner“ (Anmelde-Banner) müssen Onboard Administrator-Benutzer den Banner-Text zuerst bestätigen, bevor sie sich anmelden können.

Enable Display of Banner on User Login (Banner-Anzeige bei Benutzeranmeldung aktivieren) – Markieren Sie dieses Kontrollkästchen, um die Option „Login Banner“ (Anmelde-Banner) zu aktivieren. Durch Bestätigung des Anmelde-Banner-Textes wird Zugriff auf alle am primären Onboard Administrator angeschlossenen Systeme gewährt.

Banner Text (Banner-Text) – Die Feldgröße ist auf 1.500 druckbare Zeichen eingeschränkt, ausschließlich der Zeichen % \ < > ( ) & #. Leerstellen und Zeilenvorschübe werden zwar akzeptiert, die Verwendung von nur Leerzeichen innerhalb dieses Textfeldes ist jedoch nicht zulässig.

HINWEIS: Das Anmelde-Banner akzeptiert nur englische (ASCII) Zeichen.

Apply (Übernehmen) – Klicken Sie hier, um das Feld „Banner Text“ (Banner-Text) zu bestätigen. Wenn das Feld „Banner Text“ (Banner-Text) leer ist oder nur Leerzeichen enthält, das Kontrollkästchen „Enable Display of Banner on User Login“ (Banner-Anzeige bei Benutzeranmeldung aktivieren) jedoch aktiviert ist, werden Sie zum Deaktivieren dieser Funktion aufgefordert.

Link Loss Failover (Failover bei Verbindungsverlust)

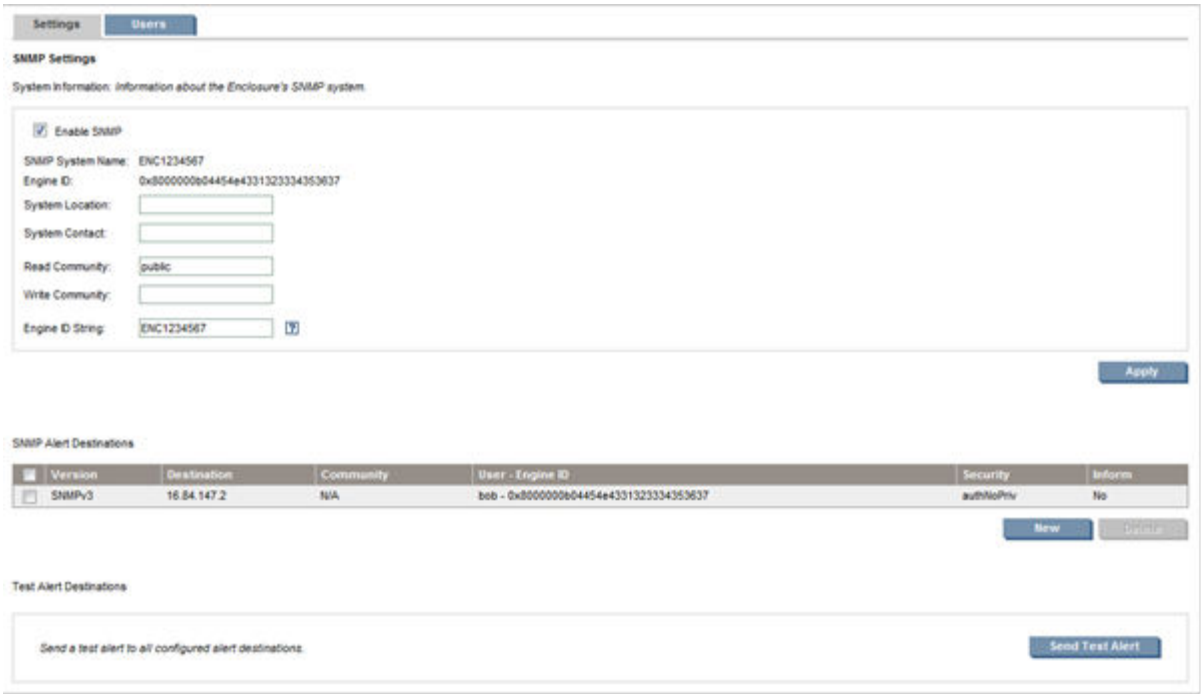
Auf diesem Bildschirm können Sie das automatische Failover für Onboard Administrator-Redundanz basierend auf dem Netzwerkverbindungsstatus konfigurieren. Das Failover bei Verbindungsverlust kann nur richtig funktionieren, wenn der Redundanzstatus der Onboard Administrator-Module „OK“ lautet. Der Status „OK“ bedeutet, dass beide Onboard Administrator-Module über die gleiche Firmwareversion (Version 2.20 oder höher) verfügen und ordnungsgemäß kommunizieren.

Enable Link Loss Failover (Failover bei Verbindungsverlust aktivieren): Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Failover bei Verbindungsverlust.

Failover Interval (Failover-Intervall): Das Failover-Intervall ist die Zeitspanne, über die hinweg das aktive Onboard Administrator-Modul ohne eine Verbindung auf der externen Ethernet-Schnittstelle erkannt werden muss, damit das System ein automatisches Failover einleitet. Das Intervall muss zwischen 30 und 86400 Sekunden lang sein.

Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

SNMP-Einstellungen



SNMP ist ein Protokoll, mit dem Verwaltungsinformationen zwischen Netzwerk-Management-Anwendungen und HP BladeSystem Onboard Administrator kommuniziert werden. Onboard Administrator unterstützt SNMP Version 1, Version 2 und Version 3 sowie einige Gruppen der Standard-MIB-II-MIB. Darüber hinaus sind weitere Informationen zur Gehäuse-Infrastruktur in der HP Rack-Informationen-MIB verfügbar. Die Rack-Informations-MIB (CPQRACK-MIB) ist Teil der Insight Management MIBs und befindet sich auf der Management CD im ProLiant Essentials Foundation Pack.

SNMPv3 unterstützt die Verschlüsselung der Agentendaten über DES oder AES128 mittels eines vom Benutzer angegebenen Kennworts. Es wird ein dedizierter Satz von SNMP-Benutzern gepflegt, jeweils mit einem Satz von Kennwörtern für Autorisierung und Authentifizierung, zusammen mit einem weiteren Satz von benutzerspezifischen Berechtigungen.

Der Bildschirm „SNMP Settings“ (SNMP-Einstellungen) ermöglicht die Eingabe von Systeminformationen und Community-Strings sowie die Angabe der Managementstationen, die SNMP-Traps von Onboard Administrator empfangen können. Wenn Sie **Enable SNMP** (SNMP aktivieren) wählen, antwortet Onboard Administrator auf SNMP-Anfragen über UDP-Port 162. Port 162 ist der UDP-Port, der standardmäßig für das Senden und Abrufen von SNMP-Nachrichten verwendet wird.

In der Unterkategorie „System Information“ (Systeminformationen) können Informationen zum SNMP-System von Onboard Administrator aktiviert und konfiguriert werden.

Das Kontrollkästchen „Enable SNMP“ (SNMP aktivieren) ist standardmäßig nicht aktiviert. Wenn dieses Kontrollkästchen aktiviert ist, kann Onboard Administrator nach Status- und einfachen Informationen abgefragt werden. Der SNMP-Client kann SNMP-Warnmeldungen und Statuszustände nur löschen, wenn der Schreib-Community-String aktiviert ist. Um den SNMP-Zugriff auf den Onboard Administrator zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Enable SNMP** (SNMP aktivieren).

HINWEIS: Im FIPS-Modus ON/DEBUG sind SNMPv1 und SNMPv2 deaktiviert. Sie können nur SNMPv3-Traps erstellen.

Feld	Möglicher Wert	Beschreibung
System Location (Systemstandort)	0 bis 20 Zeichen, darunter alle druckbaren Zeichen und die Leerstelle.	Der SNMP-Standort des Gehäuses, der in der Regel zur Identifizierung des physischen oder topografischen Standorts von Onboard Administrator verwendet wird.
System Contact (Kontaktperson für das System)	0 bis 20 Zeichen, darunter alle druckbaren Zeichen und die Leerstelle.	Der Name der Kontaktperson für das System; wird zur Identifizierung einer Person oder einer Gruppe von Personen verwendet, die im Falle einer Statusänderung in HP BladeSystem Onboard Administrator zu kontaktieren sind.
Read Community	0 bis 20 Zeichen, darunter alle druckbaren Zeichen und die Leerstelle.	Mithilfe der Zeichenfolge „Read Community“ (Community lesen) kann der Client Informationen lesen, die Mitteilungen oder den Status von HP BladeSystem Onboard Administrator über SNMPv1 oder SNMPv2 jedoch nicht ändern. Der Standard-Community-Name lautet „public“ (öffentlich) und ermöglicht den Empfang von Benachrichtigungs-Traps und Meldungen durch den Benutzer, lässt jedoch keine Änderung oder Bearbeitung des Status zu.
Write Community	0 bis 20 Zeichen, darunter alle druckbaren Zeichen und die Leerstelle.	Mithilfe der Zeichenfolge „Write Community“ (Community schreiben) kann der Client Meldungen über den Status von HP BladeSystem Onboard Administrator über SNMPv1 oder SNMPv2 bearbeiten. Sie können Meldungen über den SNMP-Management-Client mithilfe der SNMP-Agenten remote löschen und sie als „viewed“ (gelesen) oder anderweitig markieren.
Engine ID String (Modul-ID-Zeichenfolge)	Mit 1 bis 27 druckbaren Zeichen ist die endgültige Modul-ID eine hexadezimale Zeichenfolge, die mit „0x“' beginnt und von dieser Zeichenfolge abgeleitet ist.	Die Modul-ID-Zeichenfolge wird zur Erstellung des hexadezimalen Werts der Modul-ID verwendet. Die Modul-ID wird mit dem Benutzernamen kombiniert, um einen SNMPv3-Benutzer für jedes Gehäuse zu erstellen. Wenn die Modul-ID für ein Gehäuse eindeutig ist, sind Benutzer mit dem gleichen Namen für verschiedene Gehäuse eindeutig. Die Modul-ID-Zeichenfolge ist standardmäßig die Seriennummer des Gehäuses.

Nachdem ein Feld in dieser Subkategorie bearbeitet wurde, klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Hinzufügen von SNMP-Benachrichtigungszielen

Um ein aktuelles SNMP-Benachrichtigungsziel zu entfernen, markieren Sie das Kontrollkästchen und klicken Sie auf **Delete** (Löschen).

Um ein neues SNMP-Benachrichtigungsziel hinzuzufügen, klicken Sie auf **New** (Neu). Der Bildschirm „Add SNMP Alert“ (SNMP-Benachrichtigung hinzufügen) wird angezeigt.

Um einen SNMP-Test-Trap an alle konfigurierten Trap-Ziele zu senden, klicken Sie auf **Send Test Alert** (Testbenachrichtigung senden). Zur Verwendung dieser Funktion müssen Sie SNMP aktivieren.

Verwenden Sie die folgenden Felder, um die Informationen für die neue SNMP-Benachrichtigung einzugeben.

Feld	Möglicher Wert	Beschreibung
Alert Destination (Benachrichtigungsziel)	Protokoll: • udp – für IPv4-UDP-Traps • udp6 oder udpv6 oder udpipv6 – für IPv6-UDP-Traps • tcp – für IPv4-TCP-Traps (nur für SNMPv3) • tcp6 oder tcpv6 oder tcpipv6 – für IPv6-TCP-Traps (nur für SNMPv3) Ziel: • IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-	Die IP-Adresse oder der DNS-Name der Management-Station. Das Benachrichtigungsziel kann im Format [protocol:]destination[:port] ([Protokoll:]Ziel[:Port]) angegeben werden. Sowohl der Protokoll- als auch der Portparameter sind optionale Parameter.

Feld	Möglicher Wert	Beschreibung
	Adresse wird ebenfalls unterstützt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller alphanumerischen Zeichen und des Bindestrichs (-). Port: Die Portnummer kann jede gültige und verfügbare UDP/TCP-Portnummer im Bereich von [1.65535] sein (beide einschließlich). Wenn ein Port für eine IPv6-Adresse angegeben wurde, muss die IPv6-Adresse in [...] eingeschlossen sein; beispielsweise [####:####::####]: 162, um Port 162 anzugeben.	
Community String	0 bis 20 Zeichen, darunter alle druckbaren Zeichen und die Leerstelle.	Eine Textzeichenfolge, die als Kennwort fungiert. Sie wird zur Authentifizierung der Mitteilungen verwendet, die zwischen HP, dem Management-Server und Onboard Administrator gesendet werden.

HINWEIS: Im FIPS-Modus ON/DEBUG sind SNMPv1 und SNMPv2 deaktiviert. Sie können nur SNMPv3-Traps erstellen.

Um die folgenden Felder zu konfigurieren, markieren Sie das Kontrollkästchen „SNMPv3“:

- **User** (Benutzer) – das SNMP-Benutzerkonto, das zum Senden von trap/inform verwendet wird. Die gewünschte Benutzer-Modul-ID muss erstellt werden, bevor das Benachrichtigungsziel hinzugefügt werden kann.
- **Security** (Sicherheit) – die Sicherheitsstufe, die für das Senden von trap/inform verwendet wird. Sicherheitsstufenoptionen: keine Autorisierung oder Verschlüsselung (noAuthNoPriv), Autorisierung, jedoch keine Verschlüsselung (authNoPriv) sowie Autorisierung und Verschlüsselung (authPriv). Der Standardwert ist authNoPriv.
- **Inform Message** (Inform-Mitteilung) – Wenn eine „Inform Message“ (Inform-Mitteilung) festgelegt wird, erwartet der Agent eine Benachrichtigung von der Management-Anwendung, dass das Trap empfangen wurde Der Agent wiederholt das Senden des Traps, wenn er keine Inform-Bestätigung erhält. Benachrichtigungen mit aktivierter „Inform Message“ (Inform-Mitteilung) müssen über einen Remote-Benutzer verfügen, der in einer Management-Lösung verfügbar ist.

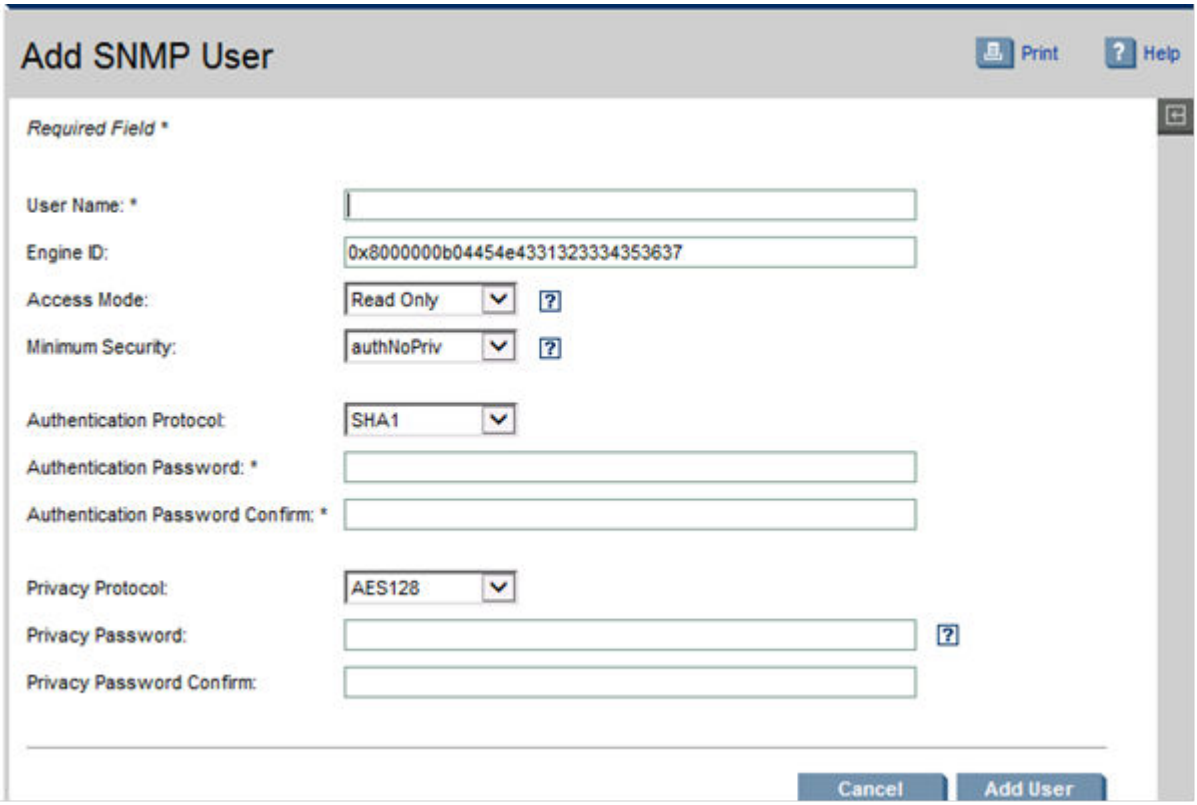
Um mit dem Hinzufügen der SNMP-Benachrichtigung fortzufahren, klicken Sie auf **Add Alert** (Alarm hinzufügen).

Registerkarte „SNMP Users“ (SNMP-Benutzer)

Um einen aktuellen SNMP-Benutzer zu entfernen, markieren Sie das Kontrollkästchen und klicken Sie auf **Delete** (Löschen).

Um einen neuen SNMP-Benutzer hinzuzufügen, klicken Sie auf **New** (Neu). Der Bildschirm „Add SNMP User“ (SNMP-Benutzer hinzufügen) wird angezeigt.

Hinzufügen von SNMP-Benutzern



Verwenden Sie die folgenden Felder, um die Informationen für den neuen SNMP-Benutzer einzugeben.

Feld	Möglicher Wert	Beschreibung
User Name (Benutzername)	Eine eindeutige Zeichenfolge mit 1 bis 32 Zeichen. Als Zeichen dürfen nur alphanumerische Zeichen, Bindestriche oder Unterstriche verwendet werden. Außerdem muss	Name des Benutzerkontos, das für SNMPv3-Abfragen, Traps und Inform-Mitteilungen verwendet wird. Jede Kombination aus Benutzername und Modul-ID muss eindeutig sein und darf nicht dupliziert werden.

Feld	Möglicher Wert	Beschreibung
	das erste Zeichen ein Buchstabe sein.	
Engine ID (Modul-ID)	Muss mit „0x“ beginnen, gefolgt von einer geraden Zahl aus bis zu 64 hexadezimalen Ziffern.	Die Modul-ID wird mit dem Benutzernamen kombiniert, um einen SNMPv3-Benutzer für jedes Gehäuse zu erstellen. Wenn die Modul-ID für ein Gehäuse eindeutig ist, sind Benutzer mit dem gleichen Namen für verschiedene Gehäuse eindeutig. Standardmäßig wird eine eindeutige Modul-ID für das Gehäuse verwendet. Nur zur Erstellung von Remote-Konten verwendet, die mit INFORM-Mitteilungen verwendet werden.
Access Mode (Zugriffsmodus)	• Lesezugriff • Lese-/Schreibzugriff	Gilt nur für lokale Benutzer. Legt fest, dass dieser Benutzer über Lese-/Schreibzugriff für die OID-Struktur verfügt. Wenn nichts festgelegt wird, verfügt der Benutzer lediglich über Lesezugriff.
Minimum Security (Mindestsicherheit)	• noAuthNoPriv – Lässt nicht authentifizierte Vorgänge zu • authNoPriv – Erfordert Authentifizierung • authPriv – Erfordert Verschlüsselung	Gilt nur für lokale Benutzer. Mindestsicherheitsstufe, die für den Vorgang erforderlich ist. Standardmäßig muss der Vorgang signiert, jedoch nicht verschlüsselt werden (authNoPriv).
Authentification Protocol (Authentifizierungsprotokoll)	• SHA1 • MD5	Verwenden Sie die Algorithmen MD5 oder SHA1 zusammen mit der Passphrase, um die einzelnen Vorgänge zu authentifizieren oder zu signieren. MD5 kann im FIPS-Modus nicht festgelegt werden.
Authentication Password (Kennwort für die Authentifizierung)	8 bis 40 Zeichen, einschließlich aller druckbaren Zeichen	Das mit dem Benutzer verknüpfte Kennwort.
Authentication Password Confirm (Bestätigungskennwort für die Authentifizierung)	8 bis 40 Zeichen, einschließlich aller druckbaren Zeichen	Das mit dem Benutzer verknüpfte Kennwort. Dieser Wert muss dem Wert für das Kennwort für die Authentifizierung entsprechen.
Privacy Protocol (Datenschutzprotokoll)	• AES128 • DES	Verwenden Sie die Algorithmen DES oder AES128 zusammen mit der Passphrase, um das Trap zu verschlüsseln. DES kann im FIPS-Modus nicht festgelegt werden.
Privacy Password (Kennwort für den Datenschutz)	Muss 8 bis 40 ausdruckbare Zeichen enthalten.	Wird für die Verschlüsselung von Vorgängen verwendet. Wenn nichts festgelegt wird, wird das Kennwort für die Authentifizierung verwendet.
Privacy Password Confirm (Bestätigungskennwort für den Datenschutz)	Muss 8 bis 40 ausdruckbare Zeichen enthalten.	Wird für die Verschlüsselung von Vorgängen verwendet. Wenn nichts festgelegt wird, wird das Kennwort für die Authentifizierung verwendet.

Um mit dem Hinzufügen des SNMP-Benutzers fortzufahren, klicken Sie auf **Add User** (Benutzer hinzufügen).

Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub)

Über die EBIPA-Bildschirme können feste IPv4- und IPv6-Adressen für Onboard Administrator-Gehäuseeinschübe konfiguriert werden. Mit der Onboard Administrator-EBIPA-Funktion können Sie eine feste IP-Adresse basierend auf der Einschubsnummer bereitstellen, wodurch die IP-Adresse eines bestimmten Einschubs selbst dann beibehalten wird, wenn ein Gerät ausgewechselt wird. Als

Verwaltungsschnittstelle für die in den Einschüben eingesteckten Komponenten muss DHCP eingestellt werden. EBIPA kann nur verwendet werden, wenn die Geräte zum Starten über DHCP eingestellt sind. Wenn für ein Gerät die statische IP-Adressierung konfiguriert ist, muss es zum Ändern der EBIPA-IP-Adresse in DHCP manuell neu konfiguriert werden.

HINWEIS: In der Onboard Administrator-Dokumentation werden EBIPA IP-Adressen als „feste IP-Adressen“ oder „feste DHCP-Adressen“ bezeichnet. Dies bedeutet, dass jede dieser Adressen eine IP-Adresse ist, die permanent mit einer bestimmten Einschubsnummer verknüpft ist, unabhängig davon, welches Gerät derzeit tatsächlich am Einschub angeschlossen ist.

Für die iLO-Einschübe des Server Blade sowie die Verbindungsmodul-Verwaltungseinschübe können auf verschiedene Arten IP-Adressen über das Verwaltungsnetzwerk bezogen werden: über die dynamische IP-Adressierung mittels eines DHCP-Servers, die statische IP-Adressierung, SLAAC über Routerankündigungen (nur IPv6) oder EBIPA. Wenn Ihr Netzwerk über einen DHCP-Dienst verfügt oder wenn Sie statische IP-Adressen manuell einzeln für die Server Blades-iLO- und Verbindungsmodule zuweisen möchten, überspringen Sie das Konfigurieren der Gehäuseeinschubs-IP-Adressierung.

EBIPA weist feste DHCP-IP-Adressen nur der Verwaltungsschnittstelle für Server-iLOs und Verbindungsmodule zu, die sich in dem internen Verwaltungsnetzwerk des Gehäuse befinden. EBIPA weist keine IP-Adressen für andere Komponenten im Verwaltungsnetzwerk extern des Gehäuses zu und kann nicht als DHCP-Server in Produktionsnetzwerken verwendet werden.

Für das Server Blade-iLO wird standardmäßig die DHCP-Adressierung eingestellt, die über die Netzwerkverbindung des aktiven Onboard Administrator-Moduls bezogen wird. Für Verbindungsmodule, die über eine interne Management-Netzwerkverbindung zum Onboard Administrator verfügen, kann ebenfalls standardmäßig die DHCP-Adressierung gelten.

HINWEIS: EBIPA erzwingt eindeutige IP-Adressen für alle Einschübe, sogar dann, wenn sich die Einschübe auf einem anderen VLAN befinden.

EBIPA-Konfigurationsrichtlinien

Dieser Abschnitt enthält allgemeine Konfigurationsinformationen. Spezifische Konfigurationsinformationen für IPv4 und IPv6 finden Sie unter „EBIPA für IPv4“ (EBIPA für IPv4 auf Seite 151) und „EBIPA für IPv6“ (EBIPA für IPv6 auf Seite 154).

Wenn Ihre Einrichtung die Zuweisung fester IP-Adressen bevorzugt, können Sie für die einzelnen Server Blade-iLO-Einschübe und Verbindungsmodul-Management-Einschübe eindeutige feste Adressen angeben oder einzelnen Server Blade- und Verbindungsmoduleinschüben über EBIPA einen Bereich fester IP-Adressen zuweisen. Wenn feste Adressen einzeln angegeben werden, können Subnetzmaske (IPv4), Gateway, DNS-Server, NTP-Server (IPv4-Verbindungsmodul) und Domänenname für jeden einzelnen Einschub gleich oder verschieden sein. Wenn über EBIPA ein Bereich fester Adressen zugewiesen wird, müssen Sie die erste IP-Adresse in einem Bereich und die Subnetzmaske angeben. Wenn Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen) für den betreffenden Einschub klicken, werden den unterhalb dieses Einschubs aufgelisteten Einschüben automatisch aufeinander folgende IP-Adressen zugewiesen. Die Angaben für Subnetzmaske, Gateway, DNS-Server, NTP-Server und Domänenname werden ebenfalls auf die einzelnen aufeinander folgenden Einschübe in der Liste kopiert.

Wenn Sie beispielsweise für EBIPA-Einschub 1 die IPv4-Adresse 16.100.226.21 angeben, dann werden den Einschüben 1 bis 16 mit der Funktion Autofill (Autom. ausfüllen) aufeinander folgende IP-Adressen im Bereich 16.100.226.21 bis 16.100.226.36 zugewiesen. Wenn Sie beispielsweise für Verbindungsmoduleinschub 3 16.200.139.51 angeben und die Funktion verwenden, dann werden den Verbindungsmoduleinschüben 3 bis 8 aufeinander folgende IP-Adressen im Bereich 16.200.139.51 bis 16.200.139.56 zugewiesen.

HINWEIS: Mittels der Schaltfläche **Autofill** (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt.

Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske oder ein IPv6-Subnetzpräfix an, die bzw. das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske oder eines Präfix, die bzw. das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.

Wenn Sie feste IP-Adressen für Managementprozessoren verwenden, dann können Sie mit dem Onboard Administrator-Befehl `hponcfg` das RIBCL-Skript mit den iLO-Netzwerkeinstellungen an ein iLO senden, sofern dieses iLO bereits eine IP-Adresse besitzt. EBIPA kann verwendet werden, um IP-Adressen auf iLOs zu laden, so dass mit dem Onboard Administrator-Befehl `hponcfg` Konfigurationsskripte an diese iLOs gesendet werden können. Änderungen an den iLO-Netzwerkeinstellungen führen dazu, dass dieses iLO die Netzwerkschnittstelle zurücksetzt und die aktuellen Verbindungen für einige Sekunden unterbricht.

Bei Server Blades doppelter Dichte dürfen für die Basiseinschübe (Einschub 1, 2 usw.) keine EBIPA-Einstellungen konfiguriert werden. Konfigurieren Sie die Einschübe der Seite A (1A, 2A usw.) und die Einschübe der Seite B (1B, 2B usw.). Mit der Funktion Autofill (Autom. ausfüllen) werden den Einschüben, die unterhalb des Einschubs aufgelistet werden, für den Sie die erste IP-Adresse im Bereich angeben, aufeinander folgende IP-Adressen zugewiesen (wenn Sie z. B. die IP-Adresse für Einschub 1A angeben und die Funktion Autofill (Autom. ausfüllen) anwenden, dann werden den Einschüben 2A, 3A usw. aufeinander folgende Adressen zugewiesen).

Verwenden Sie zum Konfigurieren der Verbindungsmoduleinschübe die Registerkarte **Interconnect Bays** (Verbindungsmoduleinschübe).

Um die Einstellungen anzuwenden, klicken Sie auf **Apply** (Übernehmen).

Die Server in den Geräteeinschüben rufen die Geräteeinschubs-EBIPA-Adressen innerhalb weniger Minuten automatisch ab. Die Verbindungsmodul-Switch-Module müssen jedoch manuell neu gestartet werden. Klicken Sie dazu auf jeder Onboard Administrator-Verbindungsmodul-Informationsseite auf die Schaltfläche **Virtual Power** (Virtueller Netzschalter).

ACHTUNG: Wenn für einen Servereinschub, der bereits die EBIPA-Adressierung verwendet, EBIPA-Konfigurationsänderungen vorgenommen werden, hat dies zur Folge, dass das EBIPA-konfigurierte iLO-Modul zurückgesetzt wird. ILO versucht dann, eine IP-Adresse zu beziehen. Dies kann zu einem Verlust der Konnektivität für Clients führen, die derzeit über die zuvor konfigurierte Adresse auf iLO zugreifen. Ein Verbindungsmoduleinschub wird nicht automatisch zurückgesetzt, die Konfigurationsänderungen können jedoch zu einem Verlust der Konnektivität für Clients führen, die derzeit über die zuvor konfigurierte Adresse auf das Verbindungsmodul zugreifen.

Bei einer Deaktivierung der EBIPA-konfigurierten Adressierung verlieren die betroffenen Geräte ihre aktuelle EBIPA-konfigurierte Adresse. Alle Clients, die über diese Adresse auf die Geräte zugreifen, verlieren ihre Konnektivität. Zur Sicherstellung des Client-Zugriffs sollten die Geräte über einen externen DHCP-Dienst oder durch Zuweisen einer statischen IP-Adresse mit einer Adresse konfiguriert werden.

Einrichten des Gehäuses mittels EBIPA ohne aktive Netzwerkverbindung

1. Konfigurieren Sie mit Insight Display eine statische IP für Onboard Administrator. Im Bildschirm „Enclosure Info“ (Gehäuse-Info) des Insight Display wird die Service-IP-Adresse des aktiven OA angezeigt. Schließen Sie den Client-PC an den Gehäuse-Service-Port (Gehäuse-Link-up-Anschluss) zwischen den OA-Einschüben mit einem Standard-Ethernet-Patch-Kabel an. Die

Client-PC-NIC muss für DHCP konfiguriert sein, da er ungefähr 1 Minute später eine IP-Adresse im Bereich 169.254.x.y abruft.

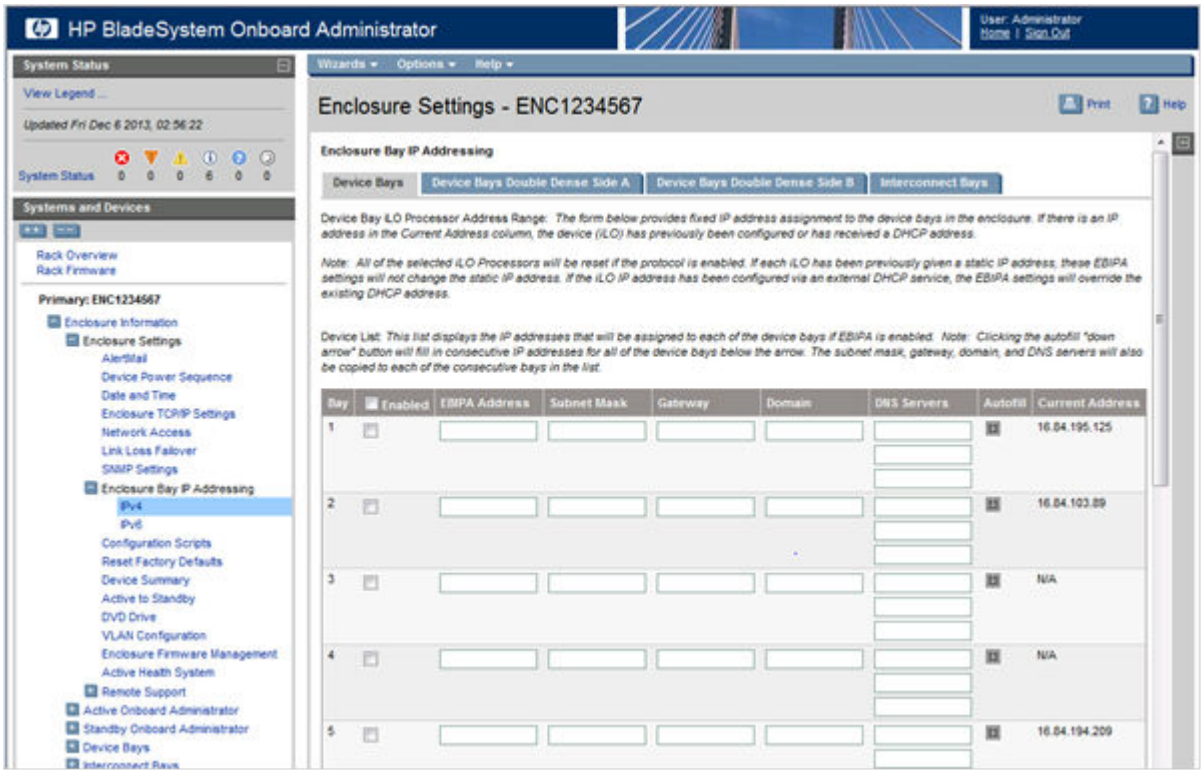
2. Starten Sie einen Web-Browser (oder alternativ eine Telnet- oder SSH-Sitzung), und wählen Sie die Onboard Administrator-Service-IP-Adresse aus, die auf dem Insight Display des Gehäuses im Bildschirm „Enclosure Info“ (Gehäuse-Info) angezeigt wird.
3. Melden Sie sich mit dem am aktiven Onboard Administrator-Modul angebrachten administrativen Kennwort als Administrator bei Onboard Administrator an.
4. Aktivieren Sie die Geräteeinschubs-EBIPA mit einer anfänglichen festen IP-Adresse, und aktivieren Sie die Verbindungsmoduleinschubs-EBIPA mit einer anderen anfänglichen IP-Adresse.

   Durch Klicken auf die Schaltfläche **Autofill** (Autom. ausfüllen) werden so viele sequenzielle, feste IP-Adressen erstellt wie erforderlich. Die Angaben für Subnetzmaske (IPv4), Gateway, DNS-Server, NTP-Server (IPv4-Verbindungsmodul) und Domänenname werden ebenfalls auf die einzelnen aufeinander folgenden Einschübe in der Liste kopiert. Alternativ dazu können Sie einzelne IP-Adressen zuweisen, indem Sie die gewünschte IP-Adresse manuell in das Feld „EBIPA Address“ (EBIPA-Adresse) für den betreffenden Einschub eingeben. Die Werte für Subnetzmaske, Gateway, DNS-Server, NTP-Server und Domänename können bei jedem einzelnen Einschub gleich oder verschieden sein.

   Nachdem die Einstellungen übernommen wurden, rufen die Server in den Geräteeinschüben die Geräteeinschubs-EBIPA-Adressen innerhalb weniger Minuten automatisch ab. Die Verbindungsmodul-Switch-Module müssen jedoch manuell neu gestartet werden. Klicken Sie dazu auf jeder Onboard Administrator-Verbindungsmodul-Informationsseite auf die Schaltfläche **Virtual Power** (Virtueller Netzschalter).
5. Überprüfen Sie anhand der Onboard Administrator-Komponentenliste, ob die Server Blade-iLO-Adressen gemäß der anfänglichen EBIPA-IP-Adresse und dem entsprechenden Bereich eingerichtet wurden.

EBIPA für IPv4

Registerkarte „EBIPA for IPv4 Device Bays“ (EBIPA für IPv4-Geräteeinschübe)


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Dec 6 2013, 02:56:22
System Status
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
Alert Mail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Device Bay iLO Processor Address Range: The form below provides fixed IP address assignment to the device bays in the enclosure. If there is an IP address in the Current Address column, the device (iLO) has previously been configured or has received a DHCP address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IP address, these EBIPA settings will not change the static IP address. If the iLO IP address has been configured via an external DHCP service, the EBIPA settings will override the existing DHCP address.
Device List: This list displays the IP addresses that will be assigned to each of the device bays if EBIPA is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IP addresses for all of the device bays below the arrow. The subnet mask, gateway, domain, and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Subnet Mask
Gateway
Domain
DNS Servers
Autofill
Current Address
1
16.84.195.125
2
16.84.103.89
3
N/A
4
N/A
5
16.84.194.209

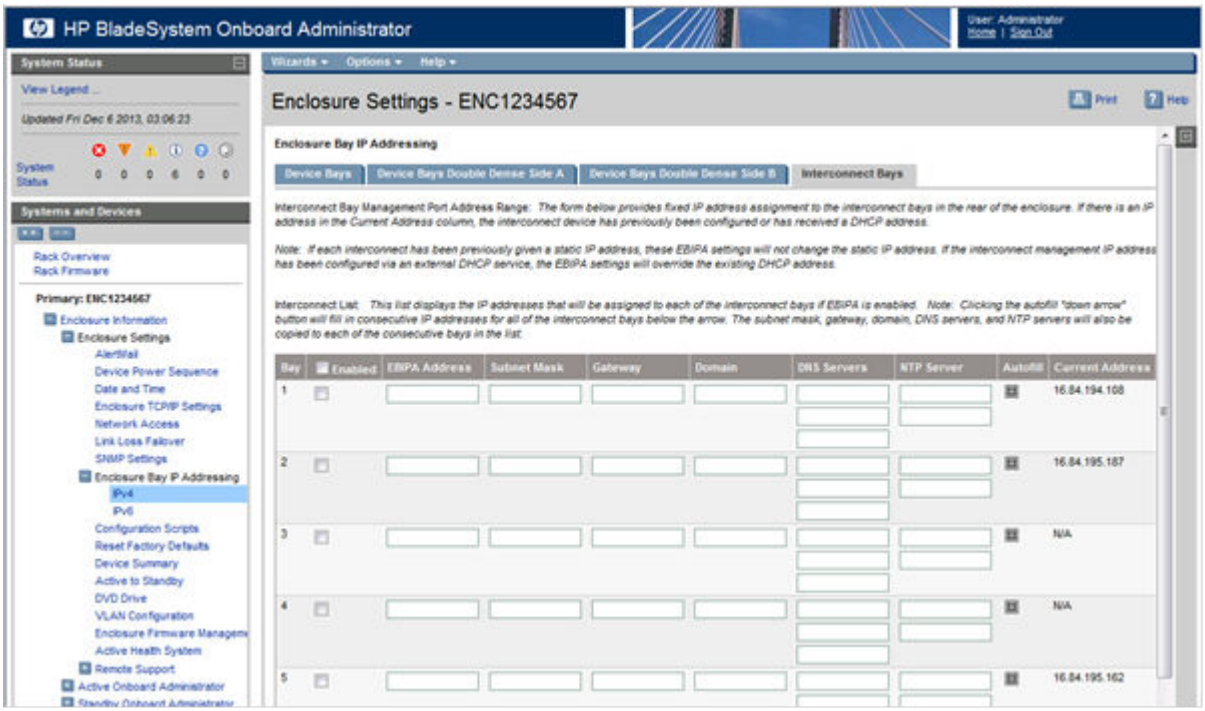
HINWEIS: Verwenden Sie beim Konfigurieren von EBIPA-zugewiesenen Adressen nicht den Bereich 169.254.x.x, da dieser Netzwerkadressbereich für den Onboard Administrator reserviert ist.

Device List (Komponentenliste)

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Komponente.
Enabled (Aktiviert)	Aktiviert EBIPA-Einstellungen für den Geräteeinschub. Durch Auswahl des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-Einstellungen für alle Geräteeinschübe aktiviert werden. Durch Auswahl des jeweiligen Kontrollkästchens für einzelne Geräteeinschübe kann der betreffende Geräteeinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste IP-Adresse, die Sie dem Geräteeinschub zuweisen möchten. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Subnet Mask (Subnetzmaske)	Subnetzmaske für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Gateway	Die feste Gateway-IP-Adresse, die Sie den Geräteeinschüben zuweisen möchten. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IP-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Autofill (Autom. ausfüllen)	Weist den unten in der Komponentenliste ausgewählten Geräteeinschüben aufeinanderfolgende IP-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen).

Spalte	Beschreibung
	Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske an, die ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske, die diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IP-Adresse des Geräteeinschubs.

Registerkarte „EBIPA for IPv4 Interconnect Bays“ (EBIPA für IPv4-Verbindungseinschübe)



Verbindungsmodulliste

HINWEIS: Verwenden Sie beim Konfigurieren von EBIPA-zugewiesenen Adressen nicht den Bereich 169.254.x.x, da dieser Netzwerkadressbereich für den Onboard Administrator reserviert ist.

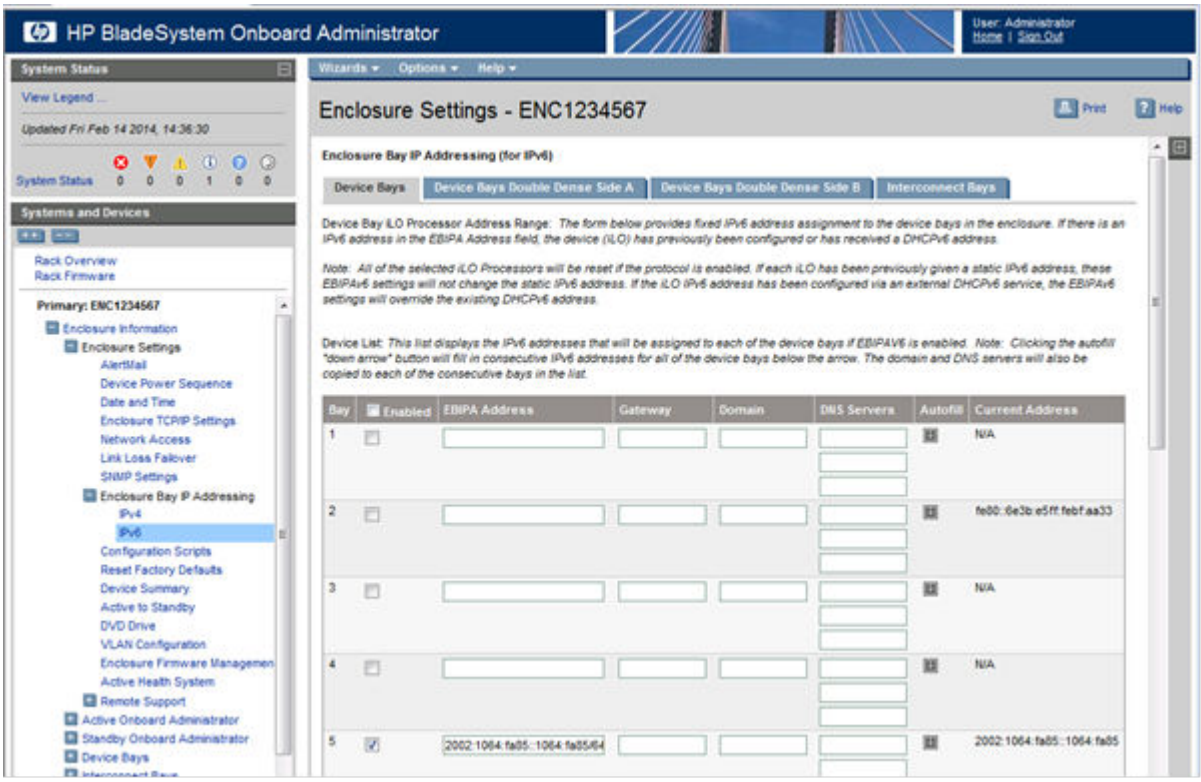
Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Verbindungsmoduls.
Enabled (Aktiviert)	Aktiviert EBIPA-für-IPv4-Einstellungen für den Verbindungsmoduleinschub. EBIPA-für-IPv4-Einstellungen für alle Verbindungsmoduleinschübe können durch Markierung des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile aktiviert werden. Durch die Markierung des jeweiligen Kontrollkästchens für einzelne Verbindungsmoduleinschübe kann der betreffende Verbindungsmoduleinschub ausgewählt werden.

Spalte	Beschreibung
EBIPA Address (EBIPA-Adresse)	Die feste DHCP-IP-Adresse, die Sie dem Geräteeinschub zuweisen möchten.
Subnet Mask (Subnetzmaske)	Subnetzmaske für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Gateway	Gateway-Adresse für die Geräteeinschübe. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv4-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt.
NTP Server (NTP-Server)	Die IPv4-Adresse des primären Servers, die für die Synchronisierung von Uhrzeit und Datum über das NTP-Protokoll verwendet wird ###.###.###.###, wobei ### im Bereich zwischen 0 und 255 liegt.
Autofill (Autom. ausfüllen)	Weist den unten in der Verbindungsmodulliste ausgewählten Verbindungsmoduleinschüben aufeinanderfolgende IPv4-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) eine IPv4-Subnetzmaske an, die ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe einer Subnetzmaske, die diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv4-Adresse des Verbindungsmoduleinschubs.

Um die EBIPA-für-IPv4-Einstellungen für die Verbindungsmoduleinschübe zu speichern, klicken Sie auf **Apply** (Übernehmen).

EBIPA für IPv6

Registerkarte „EBIPA for IPv6 Device Bays“ (EBIPA für IPv6-Geräteeinschübe)


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Feb 14 2014, 14:36:30
System Status
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing (for IPv6)
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Device Bay iLO Processor Address Range: The form below provides fixed IPv6 address assignment to the device bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.
Note: All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.
Device List: This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
N/A
2
fe80::6e3b:e5ff:febf:aa33
3
N/A
4
N/A
5
2002:1064:fa85::1064:fa85/64
2002:1064:fa85::1064:fa85

HINWEIS: Verwenden Sie beim Konfigurieren EBIPA-zugewiesener Adressen nicht das Präfix fe80::/10, da dieses Netzwerkpräfix für verbindungslokale SLAAC-Adressen reserviert ist.

HINWEIS: Damit feste EBIPA-IPv6-Adressen erfolgreich konfiguriert werden, muss die Einstellung **Enable IPv6** (IPv6 aktivieren) aktiviert sein. Sie können diese Einstellung über den Bildschirm „Network IPv6 Settings“ (Netzwerk-IPv6-Einstellungen) im „First Time Setup Wizard“ (Assistent der Erstkonfiguration) aktivieren.

Die Einstellungen **Enable SLAAC** (SLAAC aktivieren) und **Enable DHCPv6** (DHCPv6 aktivieren) wirken sich nicht auf die EBIPA-IPv6-Funktionalität aus.

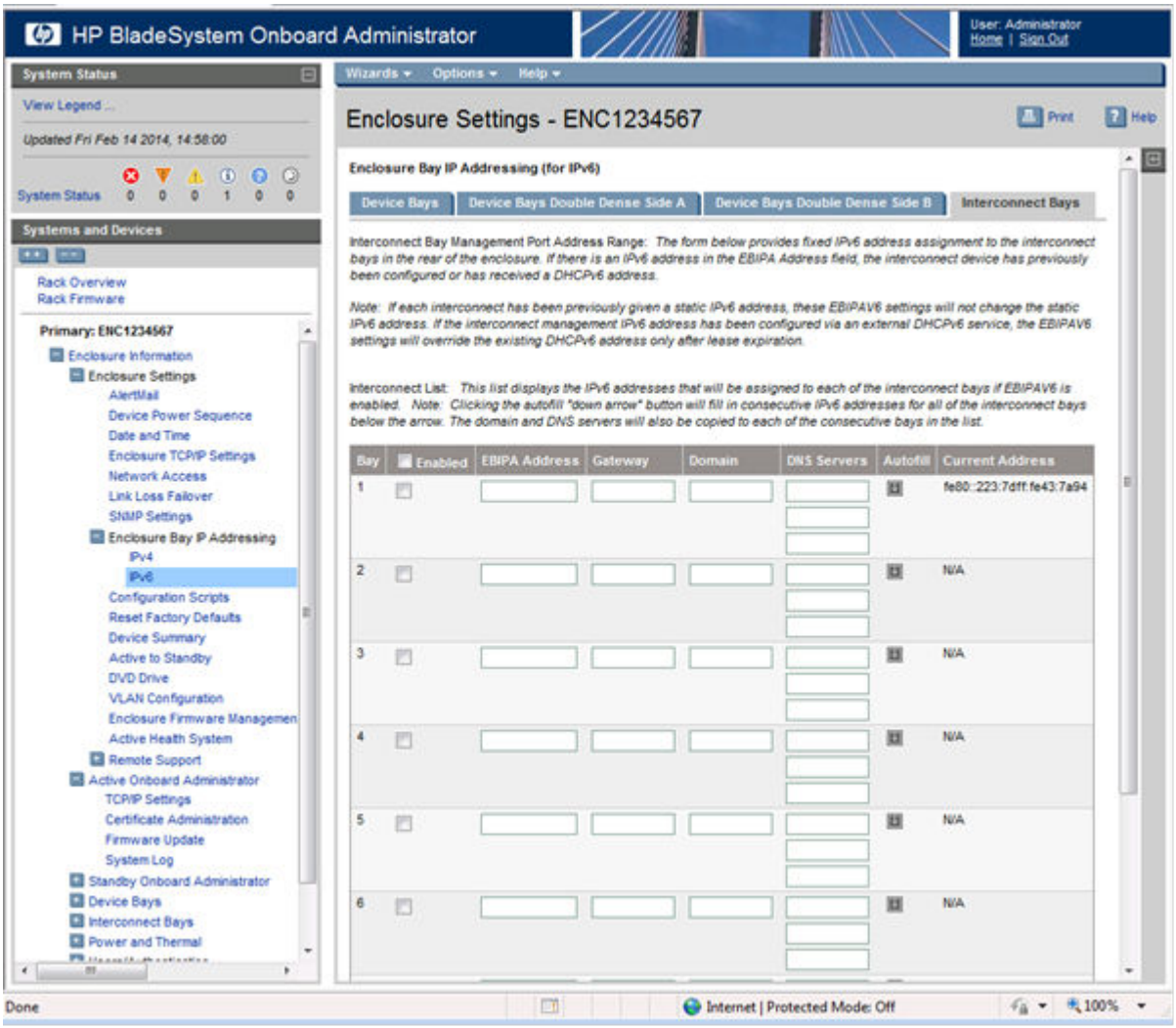
Device List (Komponentenliste)

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Komponente.
Enabled (Aktiviert)	Aktiviert EBIPA-Einstellungen für den Geräteeinschub. Durch Auswahl des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-Einstellungen für alle Geräteeinschübe aktiviert werden. Durch Auswahl des jeweiligen Kontrollkästchens für einzelne Geräteeinschübe kann der betreffende Geräteeinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste IPv6-Adresse, die Sie dem Geräteeinschub zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Das Präfix /### reicht von 1 bis 128; die Präfixlänge ist vorgeschrieben.
Gateway	Die feste IPv6-Gateway-Adresse, die Sie den Geräteeinschüben zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Geben Sie kein Präfix an. Es wird vorausgesetzt, dass das Gateway innerhalb des Netzwerks erreichbar ist.

Spalte	Beschreibung
	Wenn dieses Gateway als verbindungslokale Adresse angegeben wird, wird das Gateway immer auf dem Gehäusegerät konfiguriert, das von dieser Adresse Gebrauch macht. Wenn das Gateway mit irgendeiner anderen Art von IPv6-Adresse angegeben wird, sendet Onboard Administrator zum Identifizieren der verbindungslokalen Adresse des Gateway-Geräts, das beim Konfigurieren der Gehäusekomponenten verwendet werden soll, Nachbaranfrageaufforderungen. Wenn das Gateway nicht vorhanden ist oder nicht auf die Nachbaranfrageaufforderungen reagiert, wird kein Gateway konfiguriert.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv6-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
Autofill (Autom. ausfüllen)	Weist den unten in der Komponentenliste ausgewählten Geräteeinschüben aufeinanderfolgende IPv6-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) ein IPv6-Subnetzpräfix an, das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe eines Präfix, das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv6-Adresse des Geräteeinschubs.

Um die EBIPA-für-IPv6-Einstellungen für die Geräteeinschübe zu speichern, klicken Sie auf **Apply** (Übernehmen).

Registerkarte „EBIPA for IPv6 Interconnect Bays“ (EBIPA für IPv6-Verbindungseinschübe)


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
System Status
View Legend ...
Updated Fri Feb 14 2014, 14:58:00
System Status 0 0 0 1 0 0
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
IPv4
IPv6
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Management
Active Health System
Remote Support
Active Onboard Administrator
TCP/IP Settings
Certificate Administration
Firmware Update
System Log
Standby Onboard Administrator
Device Bays
Interconnect Bays
Power and Thermal
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Help
Enclosure Bay IP Addressing (for IPv6)
Device Bays
Device Bays Double Dense Side A
Device Bays Double Dense Side B
Interconnect Bays
Interconnect Bay Management Port Address Range: The form below provides fixed IPv6 address assignment to the interconnect bays in the rear of the enclosure. If there is an IPv6 address in the EBIPA Address field, the interconnect device has previously been configured or has received a DHCPv6 address.
Note: If each interconnect has been previously given a static IPv6 address, these EBIPAV6 settings will not change the static IPv6 address. If the interconnect management IPv6 address has been configured via an external DHCPv6 service, the EBIPAV6 settings will override the existing DHCPv6 address only after lease expiration.
Interconnect List: This list displays the IPv6 addresses that will be assigned to each of the interconnect bays if EBIPAV6 is enabled. Note: Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the interconnect bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.
Bay
Enabled
EBIPA Address
Gateway
Domain
DNS Servers
Autofill
Current Address
1
fe80::223:7dff:fe43:7a94
2
N/A
3
N/A
4
N/A
5
N/A
6
N/A
Done
Internet | Protected Mode: Off
100%

Verbindungsmodulliste

HINWEIS: Verwenden Sie beim Konfigurieren EBIPA-zugewiesener Adressen nicht das Präfix fe80::/10, da dieses Netzwerkpräfix für verbindungslokale SLAAC-Adressen reserviert ist.

Spalte	Beschreibung
Bay (Einschub)	Der Einschub im Gehäuse des Verbindungsmoduls.
Enabled (Aktiviert)	Aktiviert EBIPA-für-IPv6-Einstellungen für den Verbindungsmoduleinschub. Durch Markierung des Kontrollkästchens „Enabled“ (Aktiviert) in der Kopfzeile können EBIPA-für-IPv6-Einstellungen für alle Verbindungsmoduleinschübe aktiviert werden. Durch Markierung des jeweiligen Kontrollkästchens für einzelne Verbindungsmoduleinschübe kann der betreffende Verbindungsmoduleinschub ausgewählt werden.
EBIPA Address (EBIPA-Adresse)	Die feste DHCP-IPv6-Adresse, die Sie dem Verbindungsmoduleinschub zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####/###, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Das Präfix /### reicht von 1 bis 128; die Präfixlänge ist vorgeschrieben.
Gateway	Die feste Gateway-IPv6-Adresse, die Sie den Verbindungsmoduleinschüben zuweisen möchten. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von

Spalte	Beschreibung
	0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt. Geben Sie kein Präfix an. Es wird vorausgesetzt, dass das Gateway innerhalb des Netzwerks erreichbar ist. Wenn dieses Gateway als verbindungslokale Adresse angegeben wird, wird das Gateway immer auf dem Gehäusegerät konfiguriert, das von dieser Adresse Gebrauch macht. Wenn das Gateway mit irgendeiner anderen Art von IPv6-Adresse angegeben wird, sendet Onboard Administrator zum Identifizieren der verbindungslokalen Adresse des Gateway-Geräts, das beim Konfigurieren der Gehäusekomponenten verwendet werden soll, Nachbaranfrageaufforderungen. Wenn das Gateway nicht vorhanden ist oder nicht auf die Nachbaranfrageaufforderungen reagiert, wird kein Gateway konfiguriert.
Domain (Domäne)	Domänenname für die Geräteeinschübe. Mögliche Werte sind eine Zeichenfolge mit maximal 64 Zeichen, darunter alle alphanumerischen Zeichen, der Bindestrich (-) und der Punkt (.).
DNS Servers (DNS-Server)	IPv6-Adressen für primäre, sekundäre und tertiäre DNS-Server. Mögliche Werte sind ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.
Autofill (Autom. ausfüllen)	Weist den unten in der Verbindungsmodulliste ausgewählten Verbindungsmoduleinschüben aufeinanderfolgende IPv6-Adressen zu. Um die IP-Adressen zuzuweisen, klicken Sie auf den Abwärtspfeil **Autofill** (Autom. ausfüllen). Mittels der Schaltfläche Autofill (Autom. ausfüllen) werden nur dann alle Adressfelder ausgefüllt, wenn auf das mit der ersten Adresse in der Liste verknüpfte Adressfeld geklickt wird. Beispielsweise werden mit „Autofill“ (Autom. ausfüllen) für Adresse 1 die Adressen 1-16, mit „Autofill“ (Autom. ausfüllen) für Adresse 2 die Adressen 2-16 usw. ausgefüllt. Geben Sie bei Verwendung der Funktion „Autofill“ (Autom. ausfüllen) ein IPv6-Subnetzpräfix an, das ausreichend viele verfügbare Adressen auf dem zugehörigen Subnetz ermöglicht, so dass alle Adressfelder entsprechend der Gesamtanzahl der ausgewählten Einschübe ausgefüllt werden können. Bei Angabe eines Präfix, das diese Anforderung nicht erfüllt, wird im Adressfeld eines jeden Einschubs, für den keine Adresse erstellt werden konnte, die Meldung „Invalid IP Address“ (Ungültige IP-Adresse) angezeigt.
Current Address (Aktuelle Adresse)	Die aktuelle IPv6-Adresse des Verbindungsmduleinschubs.

Um die EBIPA-für-IPv6-Einstellungen für die Verbindungsmoduleinschübe zu speichern, klicken Sie auf **Apply** (Übernehmen).

Device Summary (Komponentenzusammenfassung)

Die FRU-Zusammenfassung enthält Informationen zu allen vor Ort austauschbaren Komponenten im Gehäuse. Die Informationen in diesem Bereich sind eine wertvolle Unterstützung für den Administrator, wenn er sich wegen Fehlerbehebung, Reparaturarbeiten oder der Bestellung von Ersatzteilen an den HP Kundendienst wendet.

Die Informationen innerhalb des Bereichs „Device Summary“ (Komponentenzusammenfassung) sind im Tabellenformat angeordnet und in Unterkategorien unterteilt:

- Enclosure
- KVM-Modul
- Onboard Administrators

- Blades
- Blade Mezzanines
- Verbindungsmodule
- Lüfter
- Netzteile

- Insight Display

Enclosure FRU Information

Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c7000 Enclosure	HP	ENC1234567	403326-B21	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	414050-001
Onboard Administrator Tray	BladeSystem c7000 Onboard Administrator Tray	HP	OI69MK0624	N/A	416000-001
Power Input Module	HP AC Module, Single Phase	HP	N/A	N/A	413494-001

Onboard Administrator FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version	Hardware Version
1	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0852	456204-B21	503826-001	3.60	B1
2	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB21BP0946	456204-B21	503826-001	3.60	B1

Blade FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	System Board Spare Part Number
1	ProLiant BL460c G1	HP	3UV839N08G	459483R-B21	438249-001
5	ProLiant BL685c G7	HP			000000-001
7	ProLiant BL460c G6	HP	MXQ923027D	507778-B21	531221-001
9	ProLiant BL460c G1	HP	USE7507R6S	447707-B21	410299-001
10	ProLiant BL460c G1	HP	USM634043S	416654-B21	410299-001
15	ProLiant BL460c G6	HP	MXQ92707MZ	507783-B21	531221-001
16	ProLiant BL460c G1	HP	USE70638DJ	404667-B21	410299-001

Blade Mezzanine FRU Information

Bay	Mezz Slot	Model	Manufacturer	Serial Number	PCA Serial Number	Part Number	Spare Part Number
1	1	NC326m Dual Port 1Gb NIC for c-Class BladeSystem	HP	CN66MK1132	CN66MK1132	406771-B21	419330-001

Interconnect FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
1	HP VC Flex-10 Enet Module	HP	TW284700YT	455880-B21	456095-001
2	HP VC Flex-10 Enet Module	HP	TW28400004	455880-B21	456095-001
6	Brocade 4/24 SAN Switch for HP c-Class BladeSystem	BROCADE	CN8625701U	AE372A	411121-001

Fan FRU Information

Bay Number	Model	Part Number	Spare Part Number
1	Active Cool 200 Fan	412140-B21	413996-001
2	Active Cool 200 Fan	412140-B21	413996-001
4	Active Cool 200 Fan	412140-B21	413996-001
5	Active Cool 200 Fan	412140-B21	413996-001
6	Active Cool 200 Fan	412140-B21	413996-001
7	Active Cool 200 Fan	412140-B21	413996-001
9	Active Cool 200 Fan	412140-B21	413996-001
10	Active Cool 200 Fan	412140-B21	413996-001

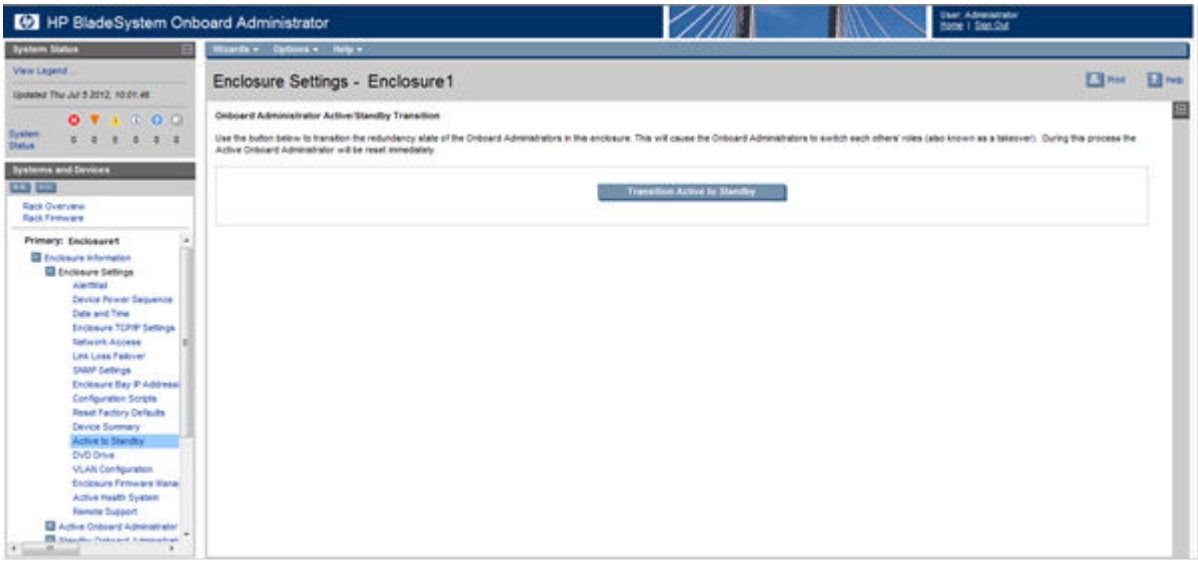
Power Supply FRU Information

Bay Number	Model	Part Number	Serial Number	Spare Part Number
1	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLU20FR	411099-001
2	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLV74LW	411099-001
3	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT4G3	411099-001
4	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLVR0AB	411099-001
5	HP BladeSystem c-Class P/S	412138-B21	5A22B0EHLUG0AD	411099-001
6	HP BladeSystem c-Class P/S	412138-B21	5A22B0DHLTT34Q	411099-001

Insight Display FRU Information

Model	Spare Part Number	Manufacturer	Firmware Version
BladeSystem c7000 LCD	415839-001	HP	2.2.2

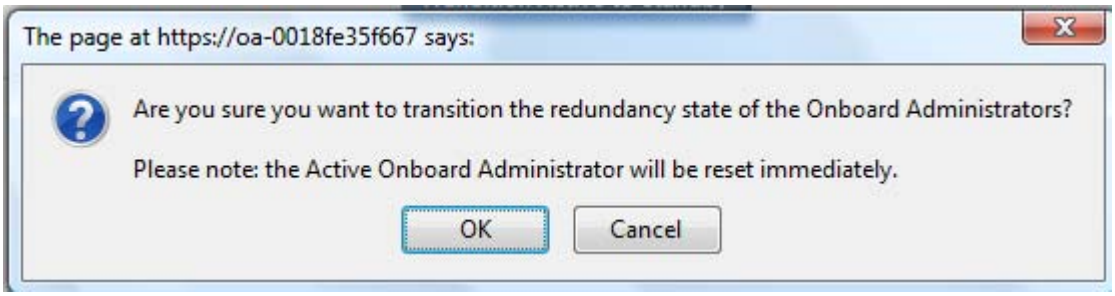
Active to Standby (Aktiv in Standby)



Wenn ein zweites HP BladeSystem-Onboard Administrator-Modul installiert ist, wird der Menüpunkt **Active to Standby** (Aktiv in Standby) unter dem Strukturmenüpunkt **Enclosure Settings** (Gehäuseeinstellungen) angezeigt, und beide Onboard Administrator-Module werden im Strukturmenü sowie in der Gehäuseansicht auf der Status-Registerkarte aufgeführt.

Wenn mehr als ein Onboard Administrator-Modul im Gehäuse installiert ist, können Sie manuell ändern, welches Onboard Administrator-Modul aktiv ist. Diese Funktion ist nützlich im Rahmen der Fehlerbehebung für Onboard Administrator oder bei Installation eines zweiten Onboard Administrator-Moduls mit einer älteren Firmwareversion (und wenn die Option für den automatischen Wechsel deaktiviert ist).

Um einen Wechsel durchzuführen, bewirken Sie durch Anklicken von **Transition Active to Standby** (Wechsel von Aktiv in Standby) die Änderung. Auf einem Bestätigungsbildschirm wird der Wechsel bestätigt und zum Schließen des Browsers aufgefordert, falls Sie beim aktiven Onboard Administrator-Modul angemeldet sind. Klicken Sie zum Fortfahren auf **OK**. Um den Vorgang ohne eine Änderung zu beenden, klicken Sie auf **Cancel** (Abbrechen).


The page at https://oa-0018fe35f667 says:
Are you sure you want to transition the redundancy state of the Onboard Administrators?
Please note: the Active Onboard Administrator will be reset immediately.
OK
Cancel

Der Wechsel kann auch mit dem Befehl `FORCE TAKEOVER` aus der Onboard Administrator-CLI vollzogen werden.

Die Dauer des Wechsels vom Standby-Modul in das aktive Modul bzw. vom aktiven Modul in das Standby-Modul ist je nach Konfiguration, Gehäuse-Bestückung und verschiedenen anderen Faktoren verschieden. Wenn das zuvor aktive Onboard Administrator-Modul während dieses Wechsels vorzeitig entfernt wird, dauert der Wechsel von „Standby“ zu „Aktiv“ länger.

DVD-Laufwerk

Auf diesem Bildschirm können Sie mehrere Server Blades im Gehäuse mit der freigegebenen DVD-Ressource verbinden, iLO Remote Console aufrufen und Befehle für den virtuellen Netzschalter auf die ausgewählten Server Blades anwenden. Die Informationen auf dieser Seite entsprechen dem letzten Download. Um die aktualisierten Informationen anzuzeigen, klicken Sie auf **Refresh** (Aktualisieren).

HINWEIS: Die Leistung von HP c-Class BladeSystem ProLiant und Integrity iLO Virtual Media wird basierend auf der Aktivität und Anzahl gleichzeitiger iLO Virtual Media-Sitzungen und der Onboard Administrator-Auslastung eingeschränkt. Die Onboard Administrator-Funktionen „Enclosure DVD Management“ (Gehäuse-DVD-Verwaltung) und „Enclosure Firmware Management“ (Gehäuse-Firmware-Verwaltung) nutzen ebenfalls die iLO-Funktion virtueller Medien und weisen ähnliche Leistungseinschränkungen auf. Um Zeitüberschreitungsprobleme der Medien zu vermeiden, empfiehlt HP, die Anzahl gleichzeitiger Sitzungen einzuschränken. Sollten während der Betriebssysteminstallation oder während Firmwareaktualisierungen Zeitüberschreitungsprobleme auftreten, dann verringern Sie die Anzahl laufender virtueller Medien-Sitzungen und starten Sie den Vorgang neu.

Spalte	Beschreibung oder Maßnahme
Kontrollkästchen	Um die Funktionen des virtuellen Netzschalters, des einmaligen Bootens oder der DVD anzuwenden, wählen Sie die Einschübe aus.
Bay (Einschub)	Dieses Feld zeigt die Geräteeinschubsnummer des Blades innerhalb des Gehäuses an.
Power State (Stromversorgungsstatus)	Der Stromversorgungsstatus des Server Blade. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
Remote Console	Um die iLO Remote Console zu starten, wählen Sie **Integrated Remote Console (IE)** oder **Remote Console Applet (Java)**, und klicken Sie dann auf **Launch** (Starten).
iLO DVD Status (ilO DVD-Status)	Dieses Feld gibt an, ob der Server Blade mit virtuellen Medien verbunden ist. Mögliche Werte sind „Connected“ (Verbunden), „Disconnected“ (Getrennt) oder „Unknown“ (Unbekannt). Lautet der Status „Inkompatible Firmware“, bedeutet dies, dass die DVD-Funktion nicht mit der auf der Komponente installierten iLO Firmware unterstützt wird. Der Status „Unknown“ (Unbekannt) weist auf ein iLO-Verbindungsproblem hin.
Device or Image URL (Komponente oder Image-URL)	Dieses Feld zeigt die aktuelle virtuelle Medienverbindung des Blades an. Mögliche Werte sind: • Standby OA DVD (Standby-OA-DVD) • Enclosure Firmware Management • Virtual Media Applet is connected (Angeschlossenes Virtual Media Applet) • Feature not supported on Integrity iLO version x.xx (Funktion auf Integrity iLO Version x.xx nicht unterstützt) • SSH is disabled on this blade's iLO processor (SSH ist auf dem iLO-Prozessor dieses Blade deaktiviert) • Upgrade ProLiant iLO 2 version x.xx to 1.30 or higher (ProLiant iLO 2 Version x.xx auf 1.30 oder höher aktualisieren) • Enclosure DVD (Gehäuse-DVD) • Tray Open or No Media (Fach geöffnet oder keine Medien) • ILO has no IP Address (ILO besitzt keine IP-Adresse)

Virtual Power (Virtueller Netzschalter)

Im Menü „Virtual Power“ (Virtueller Netzschalter) stehen die Optionen „Momentary Press“ (Kurzes Drücken) oder „Press and Hold“ (Rastendes Drücken) für den Netzschalter oder „Cold Boot“ (Kaltstart) für die ausgewählten Server Blades zur Auswahl.

Schaltfläche	Beschreibung
Momentary Press (Kurzes Drücken)	Diese Schaltfläche ahmt ein kurzes physisches Drücken des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade ordnungsgemäß ein- oder ausgeschaltet.
Press and Hold (Rastendes Drücken)	Diese Schaltfläche ahmt ein physisches Drücken und Halten des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade zum Ausschalten gezwungen, ohne zuvor das Betriebssystem herunterzufahren. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.
Cold Boot (Kaltstart)	Bei Anklicken dieser Schaltfläche wird die Stromversorgung des Systems sofort unterbrochen. Dieser Befehl gilt nur für Server Blades, die eingeschaltet sind. Die Ausgabe eines Cold Boot (Kaltstart)-Befehls an einen ausgeschalteten Server führt zum Einschalten des Server Blade.

One Time Boot (Einmaliges Booten)

Option	Beschreibung
Diskette Drive (A:) (Diskettenlaufwerk)	Bewirkt einen Neustart des Server Blade über das Diskettenlaufwerk. Vergewissern Sie sich vor Auswahl dieser Option, dass am Server Blade ein Diskettenlaufwerk angeschlossen ist.
CD-ROM	Bewirkt einen Neustart des Server Blade über das CD-ROM-Laufwerk. Vergewissern Sie sich vor Auswahl dieser Option davon, dass am Server Blade ein CD-ROM-Laufwerk angeschlossen ist.
Hard Drive C: (Festplattenlaufwerk C:)	Bewirkt den Neustart des Server Blade von der Festplatte.
RBSU	Bewirkt das Booten des Server Blade über das RBSU (ROM-Based Setup Utility).
PXE NIC	Bewirkt das Booten des Server Blade über PXE NIC.

DVD

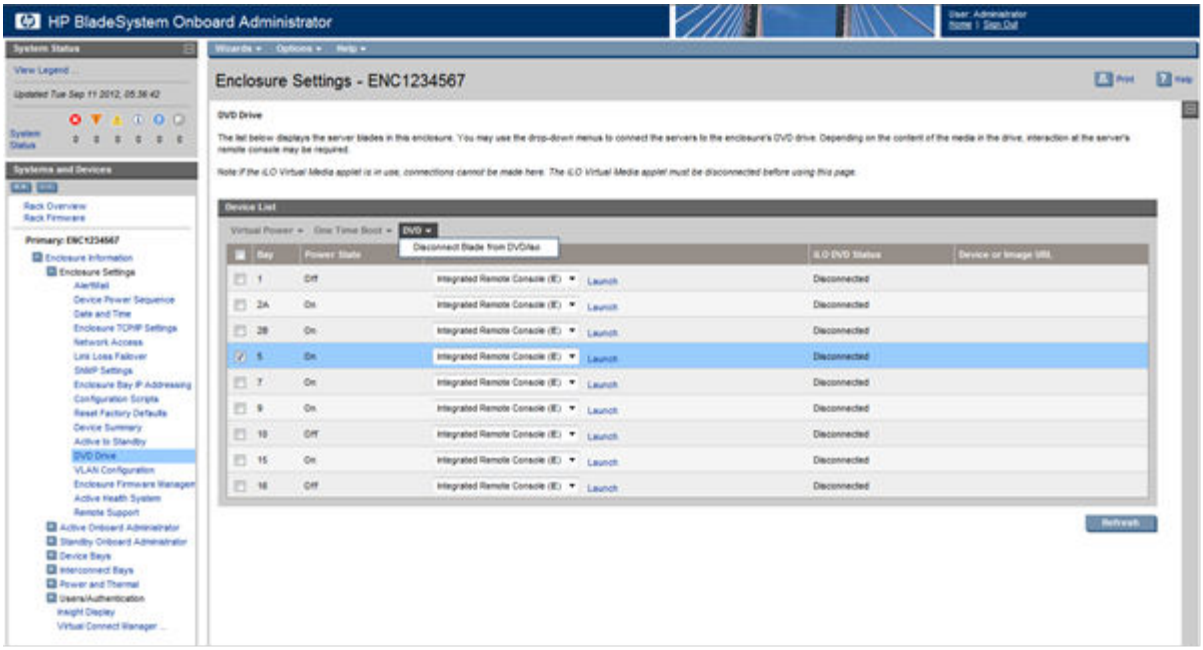
Über das Menü „DVD“ können Sie das gemeinsam genutzte DVD-Laufwerk verbinden oder trennen, indem Sie Connect to Enclosure DVD (Mit Gehäuse-DVD verbinden) bzw. Disconnect DVD Hardware (DVD-Hardware trennen) wählen. Sie können das gemeinsam genutzte DVD-Laufwerk mit mehreren Server Blades verbinden. Nachdem das freigegebene DVD-Laufwerk verbunden wurde, können Sie die in der Liste ausgewählten Server Blades über das Menü „Virtual Power“ (Virtueller Netzschalter) neu starten. Wenn für eine Installation mehrere Mediendatenträger benötigt werden, dann müssen Sie die Verbindung und Trennung möglicherweise für jeden Server durchführen, wenn der neue Mediendatenträger in das DVD-Laufwerk eingelegt wird.

Wenn ein USB-Schlüssel im USB-Port des aktiven Onboard Administrator-Moduls erkannt wird und ISO-Images vorhanden sind, werden diese im DVD-Menü angezeigt. Wählen Sie die Server Blades aus, für die Sie ein ISO-Image bereitstellen möchten, und wählen Sie dann das ISO-Image im Menü aus. Das ISO-Image wird bereitgestellt.

Interaktive Installation und Konfiguration des DVD/CD-ROM-Laufwerks

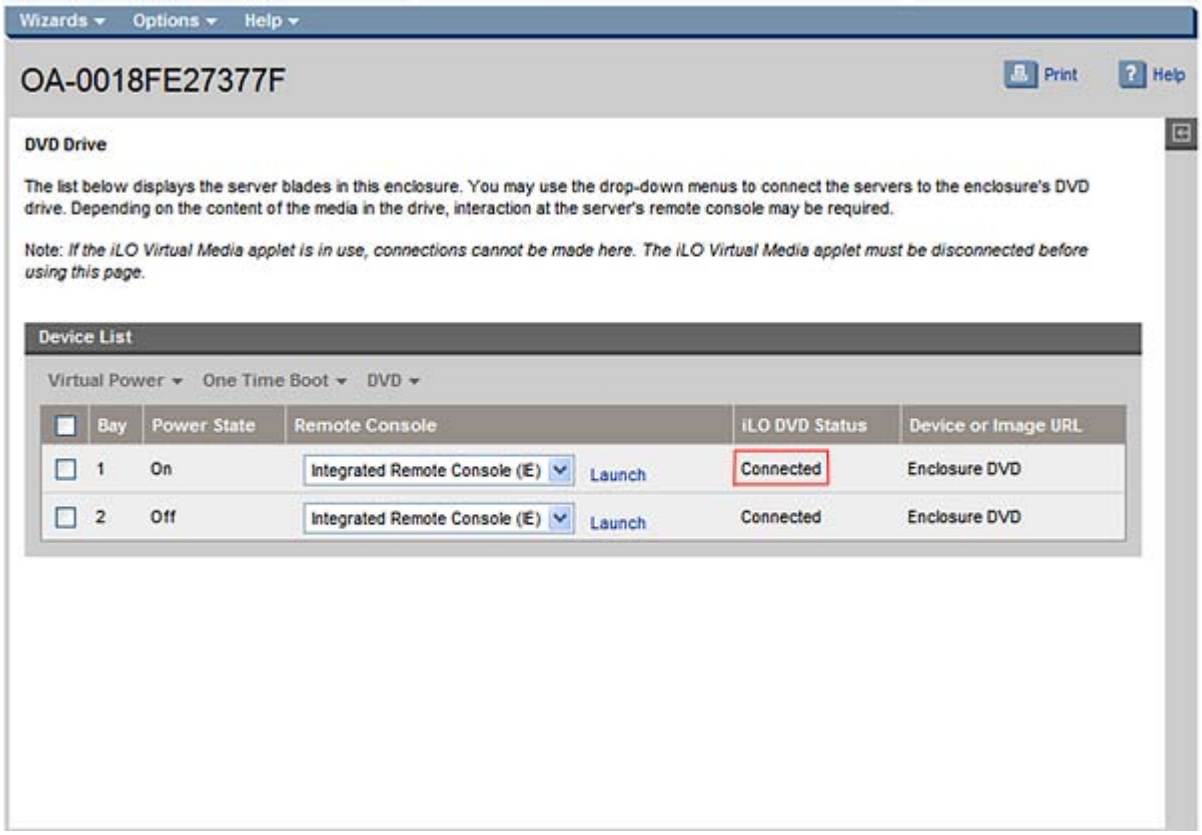
Sie können ein Blade-Betriebssystem oder eine Softwareanwendung interaktiv installieren und konfigurieren.

Blades können auf Medien im DVD-Laufwerk zugreifen, indem sie zuerst eine Verbindung zum DVD-Laufwerk herstellen und dann zur Seite „DVD Drive Summary“ (Zusammenfassung des DVD-Laufwerks) oder zur Seite „Device Bay Summary“ (Zusammenfassung des Geräteeinschubs) navigieren. Um den Zugriff auf Medien im DVD-Laufwerk zu ermöglichen, legen Sie einen Datenträger in das Laufwerk ein, wählen Sie das DVD-Menü aus, und klicken Sie dann auf **Connect to Enclosure DVD** (Mit Gehäuse-DVD verbinden).



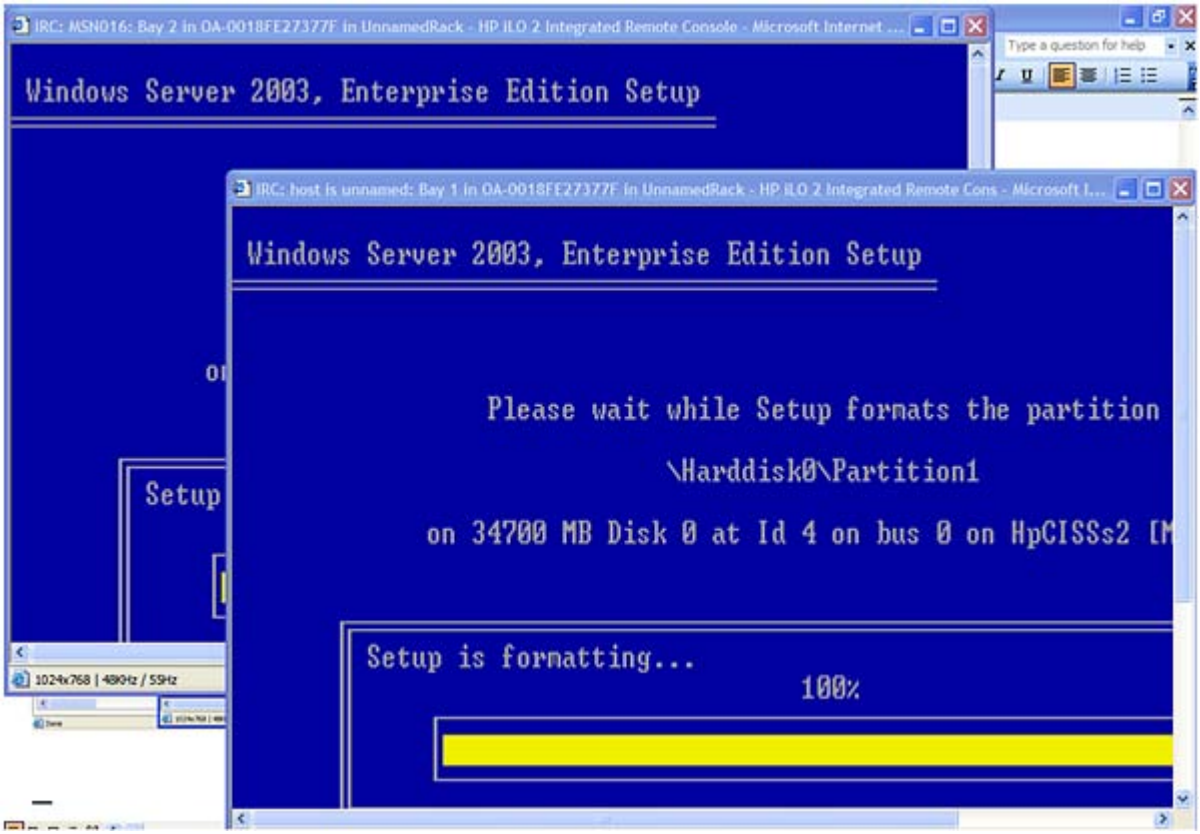
Nachdem der Datenträger im DVD-Laufwerk eingelegt wurde, können Sie den Blade mit den entsprechenden Menüoptionen auf der Seite zur Zuordnung des DVD-Laufwerks zur Geräteliste von Onboard Administrator einschalten oder neu starten. Um eine iLO Remote Console-Sitzung zu starten und die Konsole des ausgewählten Blade anzuzeigen, klicken Sie auf **Launch** (Starten). Die Leistung kann mit zunehmender Anzahl der Blades variieren.

Weitere Informationen zur Verwendung der iLO Remote Console finden Sie im iLO Benutzerhandbuch.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD
2
Off
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD

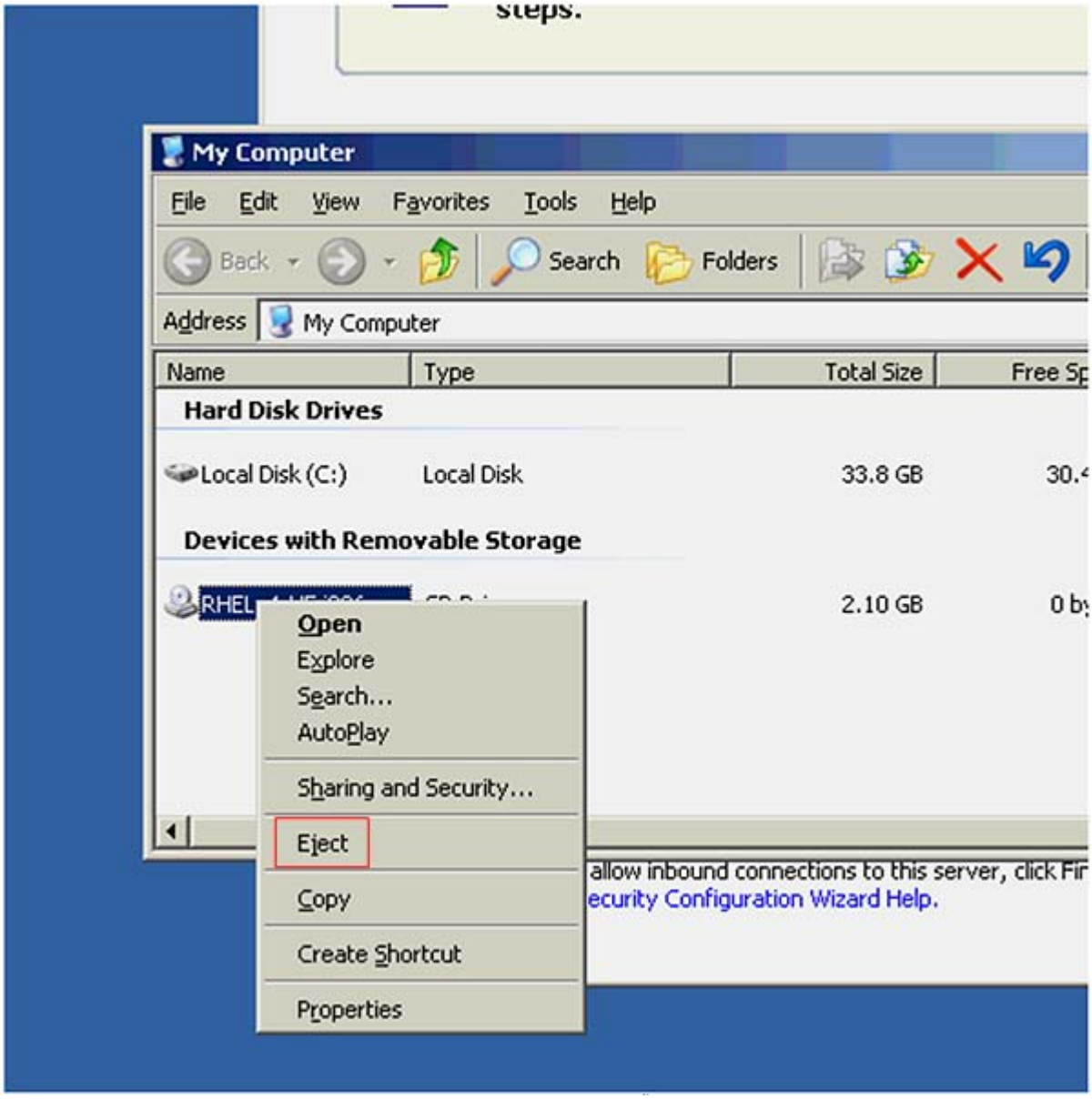
Ist im DVD-Laufwerk eine Windows®-Installations-CD eingelegt, kann der Benutzer wie unten dargestellt die Integrated Remote Console-Anzeige verwenden.

Windows Server 2003, Enterprise Edition Setup
Welcome to Setup.
This portion of the Setup program prepares Microsoft(R) Windows(R) to run on your computer.
• To set up Windows now, press ENTER.
• To repair a Windows installation using Recovery Console, press R.
• To quit Setup without installing Windows, press F3.
Windows Server® 2003 wird auf dem Blade installiert.

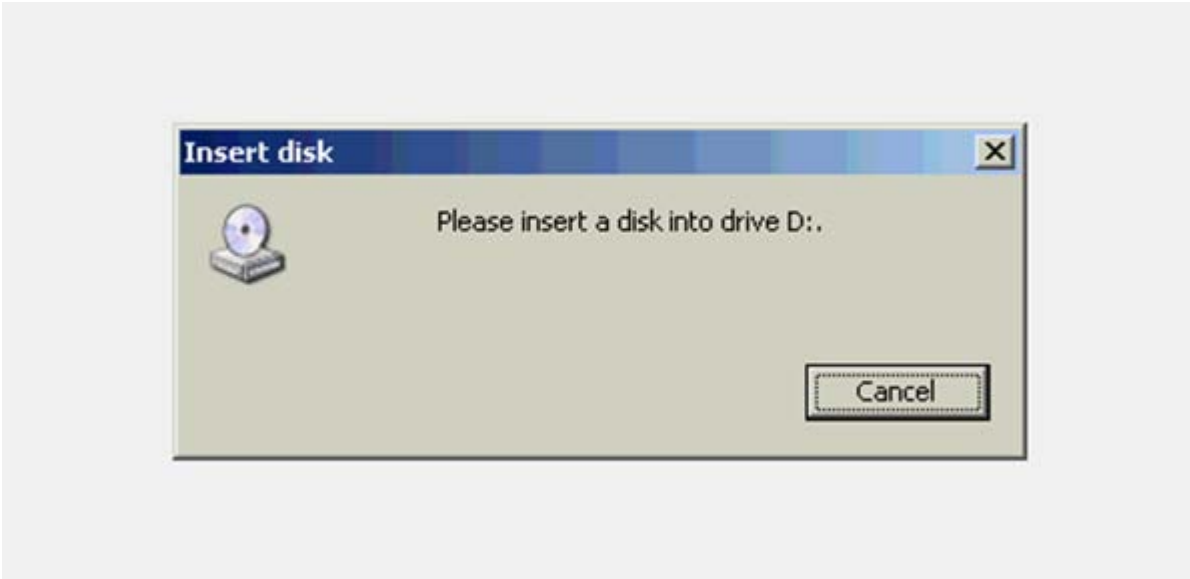

Windows Server 2003, Enterprise Edition Setup
Windows Server 2003, Enterprise Edition Setup
Please wait while Setup formats the partition
\Harddisk0\Partition1
on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2
Setup is formatting...
100%
Setup

Werfen Sie, sofern erforderlich, den Datenträger aus dem DVD-Laufwerk aus, und legen Sie den nächsten Installationsdatenträger ein. Ist das DVD-Laufwerk (mindestens 16 Sekunden lang) nicht in Betrieb, klicken Sie auf die Schaltfläche **DVD Drive Tray Open** (DVD-Laufwerksfach öffnen). Das DVD-Laufwerk des Gehäuses ist über das Fenster „IRC Virtual Media“ weder zugänglich noch steuerbar.

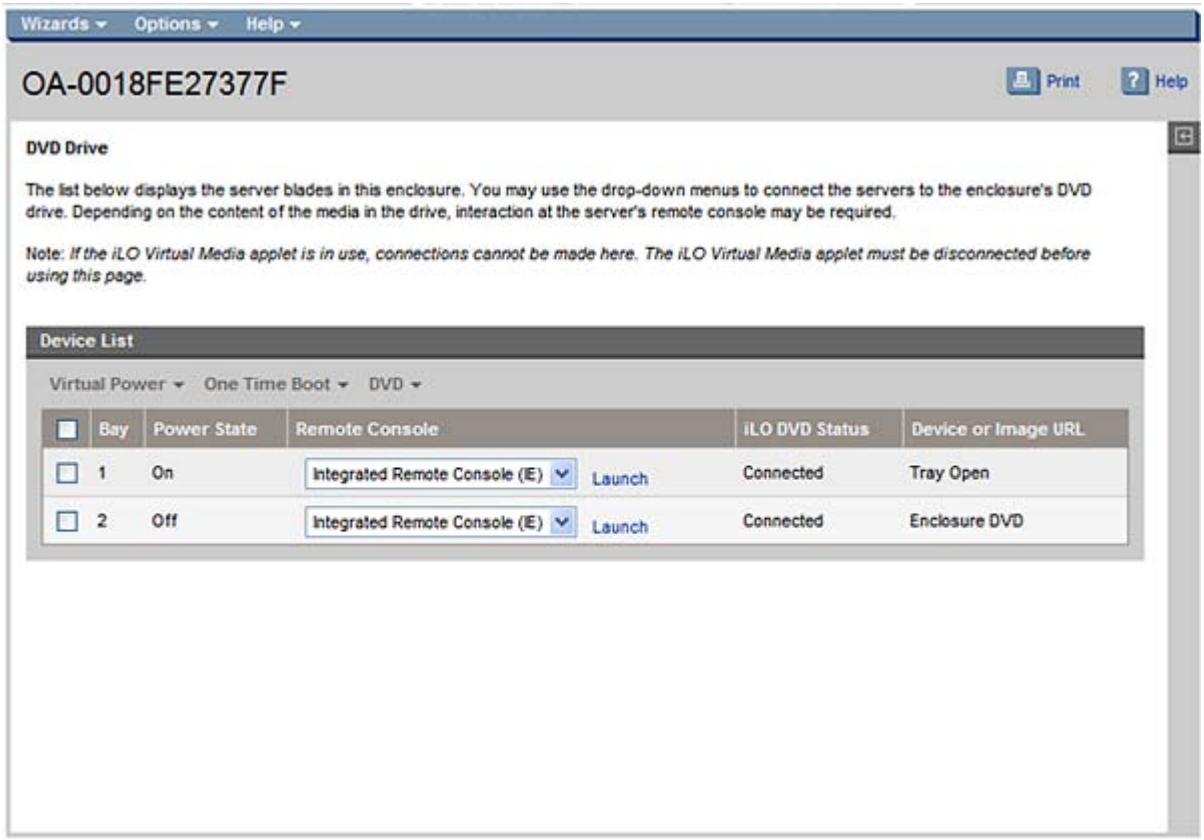
Zum Auswurf der Medien aus dem DVD-Laufwerk können Sie die Menüoption „Auswerfen“ des Betriebssystems auf dem am Laufwerk angeschlossenen Blade verwenden.



Nachdem die Medien aus dem DVD/CD-ROM-Laufwerk ausgeworfen wurden, fordert Sie das Betriebssystem zum Einlegen einer DVD oder CD auf.



Nach Ausgabe eines Auswurfbefehls vom Betriebssystem zeigt die Blade-Komponente oder das Image-URL die Meldung `Tray Open` (Fach geöffnet) an. Das physische Laufwerk wird jedoch erst nach Drücken der Taste zum Öffnen des Laufwerksfachs vorne am DVD-Laufwerk geöffnet.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (E)
Launch
Connected
Tray Open
2
Off
Integrated Remote Console (E)
Launch
Connected
Enclosure DVD

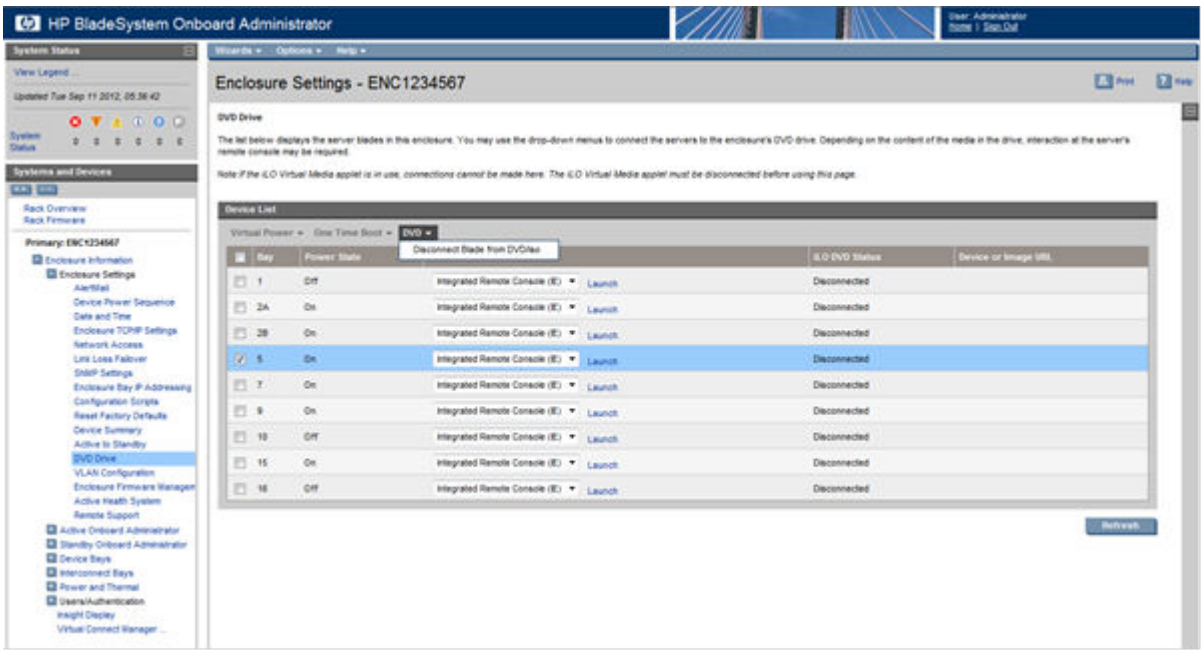
Sie können Medien je nach Bedarf des Betriebssystems, der Anwendung und der Datenanforderungsrichtlinien einlegen und auswerfen.

Unbeaufsichtigte Bereitstellung des Betriebssystems

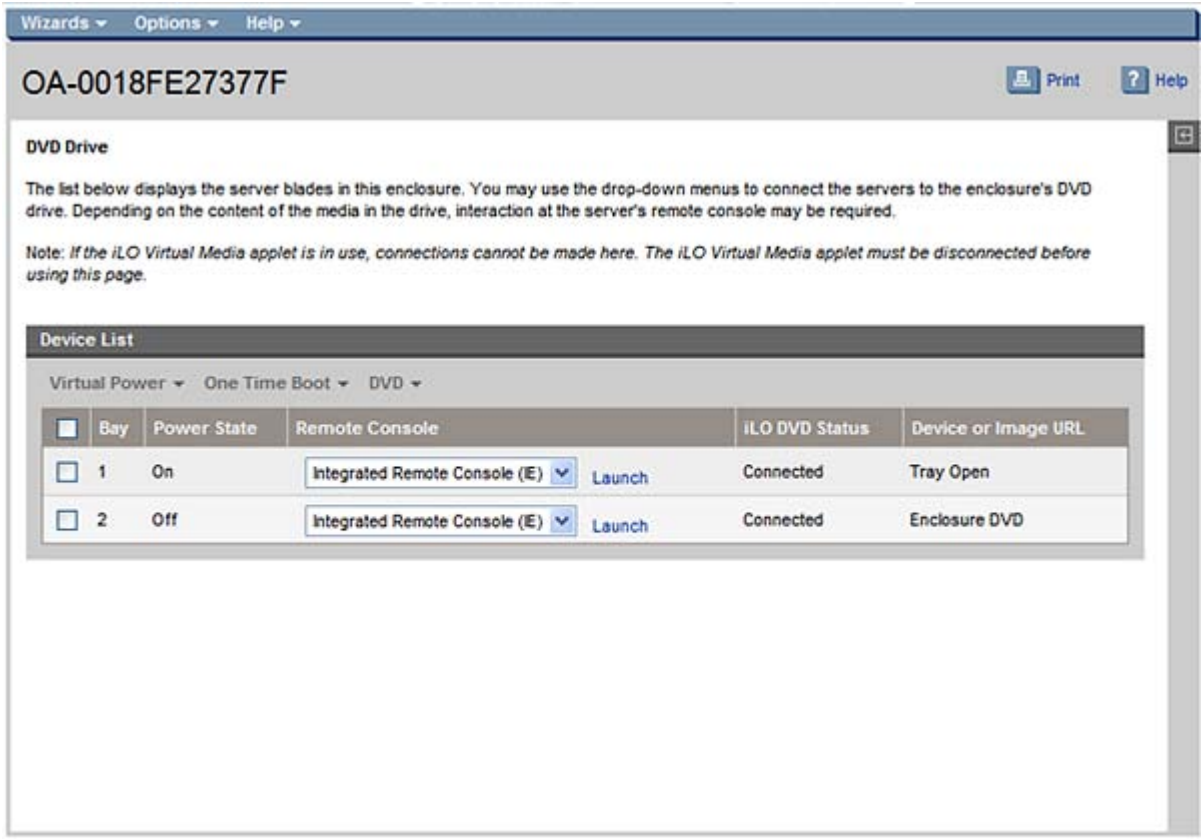
Onboard Administrator kann unbeaufsichtigt durch Nutzung des gemeinsam genutzten DVD/ROM-Laufwerks Installationen für bis zu acht Blades bereitstellen. Der Basis-Datenträger im DVD/CD-ROM-Laufwerk muss dazu fähig sein, den Blade zu booten, die Blade-Hardware zu ermitteln, lokale Festplattenpartitionen anzulegen und ein Betriebssystem auf dem Blade bereitzustellen. Für diese Art von Bereitstellung ist nur ein Datenträger erforderlich und müssen keine Medien ausgeworfen werden. Nachfolgende Anwendungen können auf die gleiche Art installiert werden, solange die Anwendung auf einen einzelnen Datenträger passt.

So greifen Sie auf Medien im DVD-Laufwerk eines Blades zu:

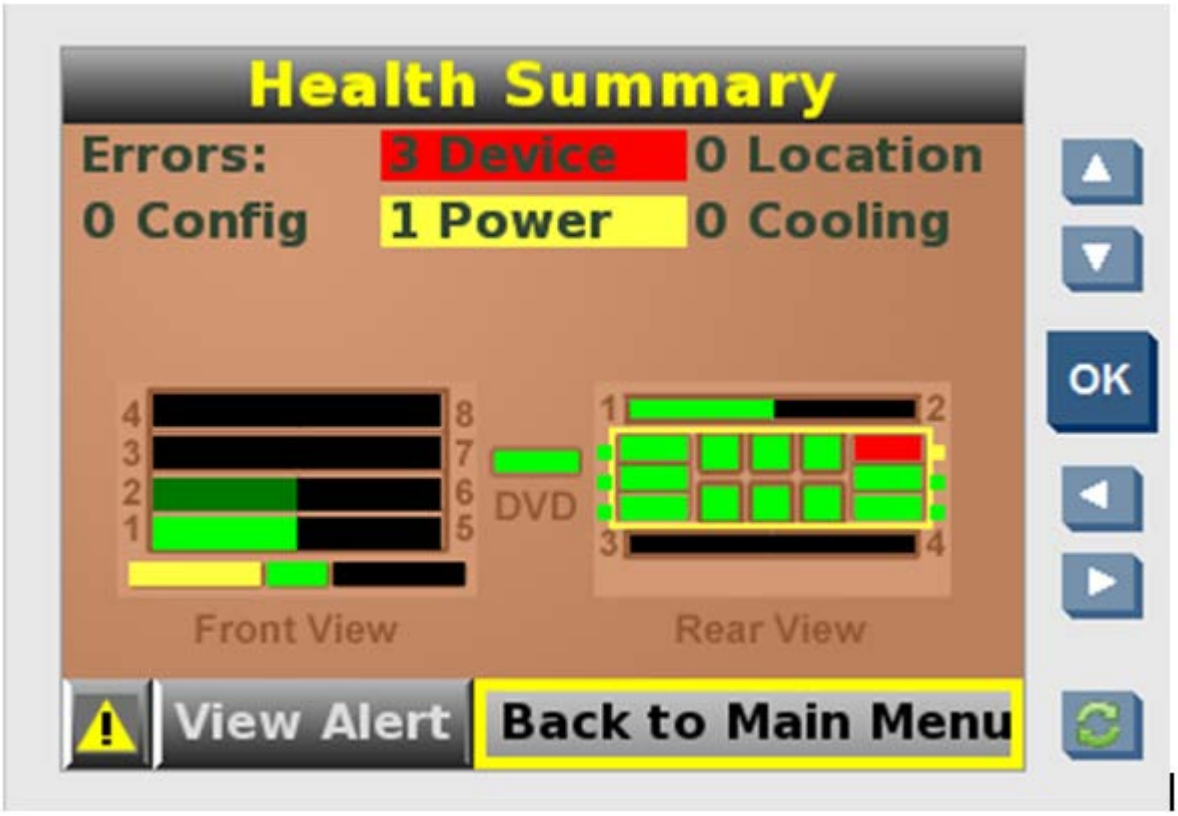
1. Verbinden Sie den Blade mit dem Laufwerk, indem Sie die Seite des DVD/CD-ROM-Laufwerks aufrufen.
2. Navigieren Sie dann zur Seite zur Zuordnung der Geräteliste.
3. Wählen Sie das DVD-Menü aus und danach **Connect to Enclosure DVD** (Mit Gehäuse-DVD verbinden) aus.
4. Legen Sie die Medien in das DVD/CD-ROM-Laufwerk ein, bevor Sie eine Verbindung zu ihm herstellen.



Nachdem die Medien in das DVD-Laufwerk eingelegt wurden, können Sie den Blade mit den entsprechenden Menüoptionen auf der Seite zur Zuordnung des DVD-Laufwerks zur Geräteliste einschalten oder neu starten.


Wizards
Options
Help
OA-0018FE27377F
Print
Help
DVD Drive
The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.
Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.
Device List
Virtual Power
One Time Boot
DVD
Bay
Power State
Remote Console
iLO DVD Status
Device or Image URL
1
On
Integrated Remote Console (IE)
Launch
Connected
Tray Open
2
Off
Integrated Remote Console (IE)
Launch
Connected
Enclosure DVD

Sie können auf dem Insight Display eine unbeaufsichtigte Bereitstellung des Betriebssystems einleiten. Um mit dem Installationsvorgang zu beginnen, schließen Sie das DVD/CD-ROM-Laufwerk an, und starten Sie dann den Server neu. Legen Sie die DVD oder CD in das DVD/CD-ROM-Laufwerk ein. Der Bildschirm „Health Summary“ (Status – Zusammenfassung) von Insight Display zeigt ein grünes Statussymbol an, woran zu erkennen ist, dass Medien eingelegt sind. Blades können nur mit dem DVD-Laufwerk verbunden werden, nachdem Medien eingelegt wurden. Die Leistung kann mit zunehmender Anzahl der Blades variieren.

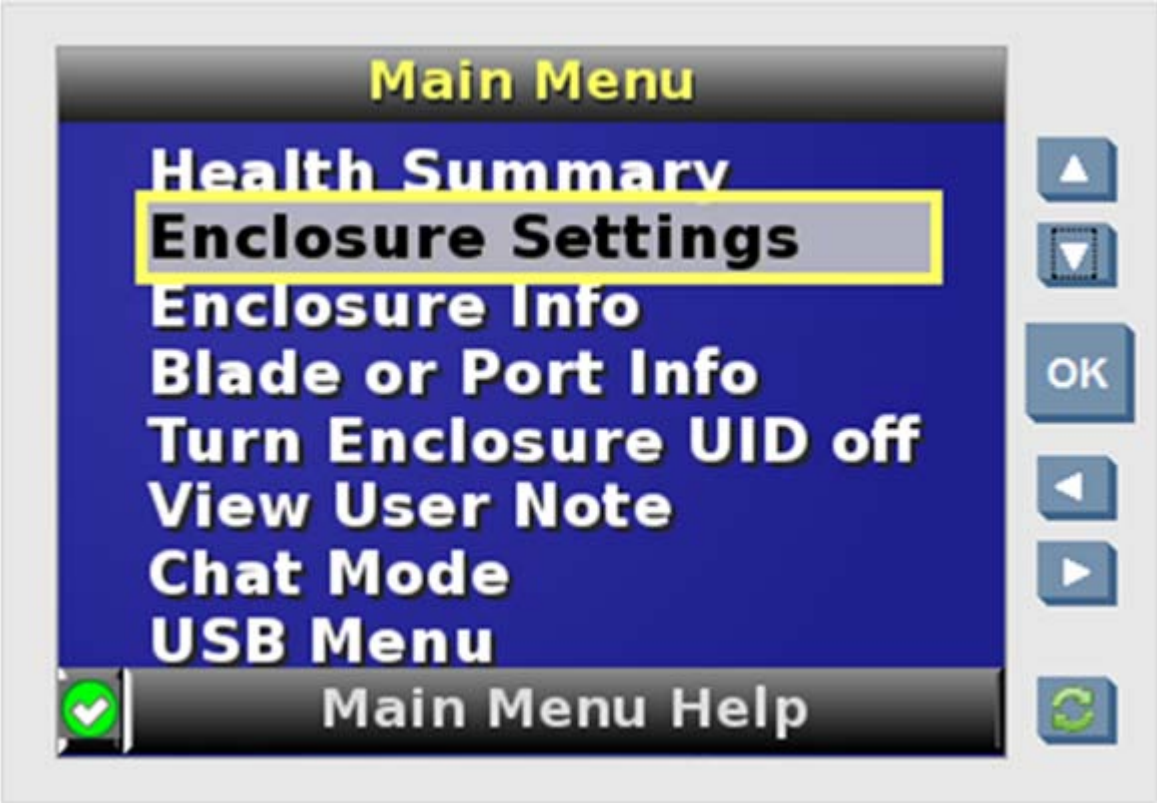


Das Insight Display zeigt den Status des DVD/CD-ROM-Laufwerks auf dem Bildschirm „Health Summary“ (Status – Zusammenfassung) als DVD-Symbol in einer der folgenden Farben an:

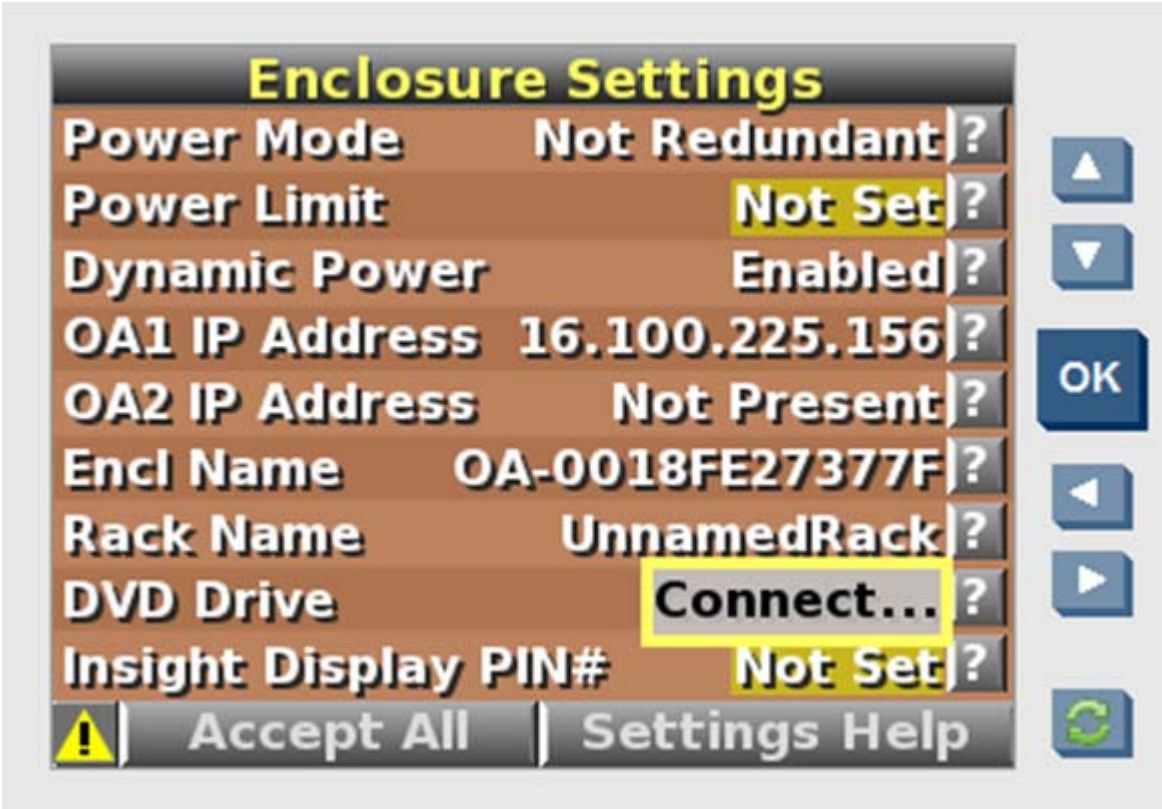
- Schwarz – Kein Laufwerk vorhanden.
- Hellgrau – Laufwerk vorhanden, aber keine Medien eingelegt.
- Dunkelgrün – Getrennte Medien vorhanden.
- Hellgrün – Verbundene Medien vorhanden.

Im Hauptmenü von Insight Display können Sie Blades mit dem DVD/CD-ROM-Laufwerk verbinden und die Blades dann neu starten.

Wählen Sie im Hauptmenü die Option **Enclosure Settings** (Gehäuseeinstellungen).



Wählen Sie im Bildschirm „DVD Drive Enclosure Settings“ (Gehäuseeinstellungen des DVD-Laufwerks) die Option **Connect...** (Verbinden…).



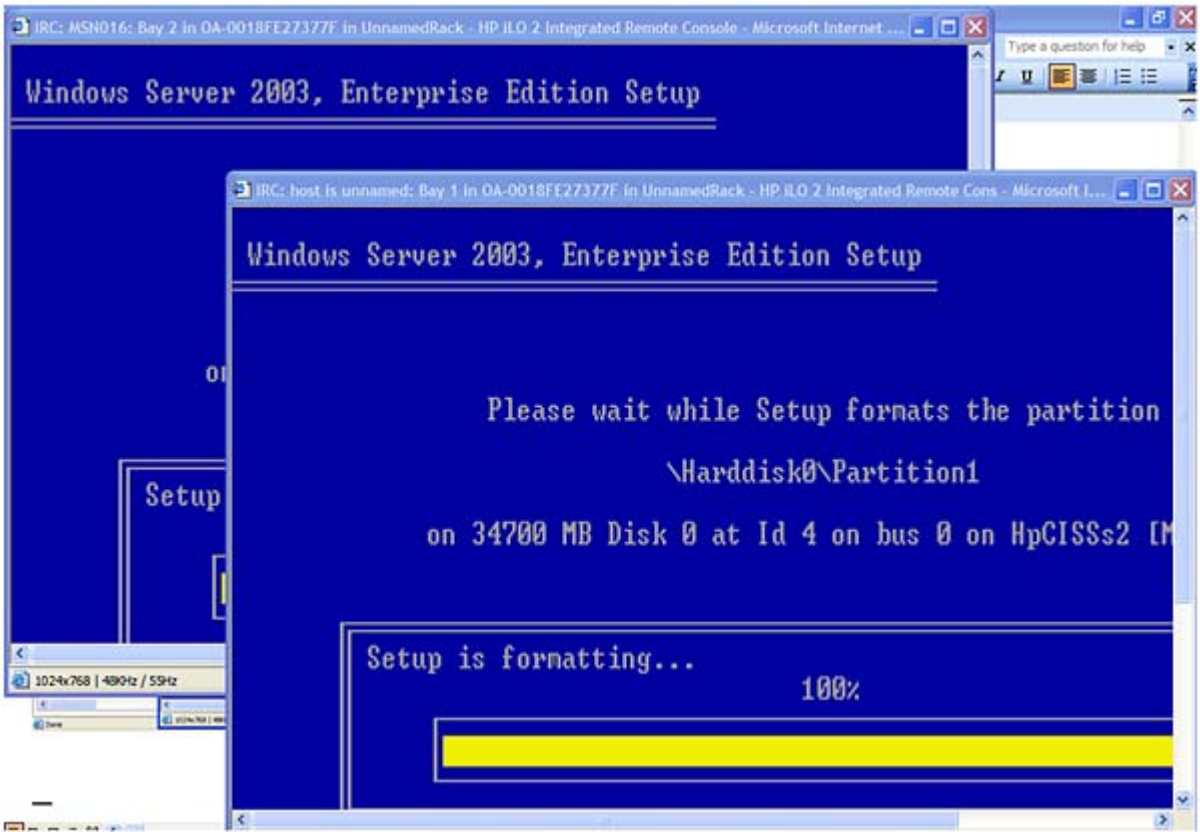
Wählen Sie auf dem Bildschirm „DVD Connection Status“ (DVD-Verbindungsstatus) **All Blades** (Alle Blades).

Wählen Sie **Connect to Enclosure DVD** (Mit Gehäuse-DVD verbinden) auf dem Bildschirm „Blade DVD Connection“ (Blade-DVD-Verbindung).

Wählen Sie im Bildschirm „Connect: Blade DVD“ (Verbinden: Blade-DVD) die Option **Connect and Reboot** (Verbinden und Neustarten) aus.

Alle Blades werden mit dem verbundenen DVD/CD-ROM-Laufwerk neu gestartet. Wenn die Medien im DVD/CD-ROM-Laufwerk startfähig sind, werden die Blades über diese Medien gestartet. Wenn eine Partition vorhanden ist, versucht der Server möglicherweise von der lokalen Festplatte zu booten. Sind die Blades älter oder wurden sie zuvor gelöscht, löschen Sie alle lokalen Laufwerkspartitionen, und erstellen Sie sie neu.

Mit der Integrated Console können Sie den Status der unbeaufsichtigten Installation anzeigen.


Windows Server 2003, Enterprise Edition Setup
Windows Server 2003, Enterprise Edition Setup
Please wait while Setup formats the partition
\Harddisk0\Partition1
on 34700 MB Disk 0 at Id 4 on bus 0 on HpCISSs2
Setup is formatting...
100%
Setup

Sofortzugriff auf DVD-basierte Medien zur Installation von Anwendungen und für den Datenimport

Sie können in das gehäusebasierte DVD/CD-ROM-Laufwerk CDs oder DVDs einlegen, um Aufgaben wie die Installation von Anwendungen oder das Laden von Daten von einer CD durchzuführen. Diese Aufgaben können nach Bedarf durchgeführt werden. Die Hauptfunktion des DVD-Laufwerks besteht nicht darin, als Startgerät zu fungieren.

Aktualisieren der Blade-Firmware mit HP Smart Update Manager

Verwenden Sie das DVD-Laufwerk des HP BladeSystem-Gehäuses und die Firmware-Wartungsmedien, um die ROMs auf allen Server Blades zu aktualisieren. Erstellen Sie die Firmwarewartungs-DVD-Medien, um eine startfähige DVD zu erstellen. Legen Sie die DVD in das gemeinsam genutzte DVD-Laufwerk ein, schließen Sie alle Server Blades an das Laufwerk an, und starten Sie sie dann neu. Die Firmwarewartungs-DVD wird auf allen am DVD-Laufwerk angeschlossenen Server Blades ausgeführt.

Weitere Informationen zum HP Smart Update Manager finden Sie im *HP Smart Update Manager User Guide* (HP Smart Update Manager Benutzerhandbuch). Weitere Informationen über das Aktualisieren der Firmware auf Server Blades finden Sie im Dokument *HP BladeSystem ProLiant*

Firmware Management Best Practices (HP BladeSystem ProLiant Firmwaremanagement – Beste Praktiken).

VLAN-Konfiguration

Onboard Administrator 3.00 und höher bietet ein vom Benutzer konfigurierbares IEEE 802.1Q-getaggtes VLAN. Diese Funktion ermöglicht Ihnen, den Datenverkehr vom Server oder vom Verbindungsmodul völlig zu isolieren, indem Sie auf dem Gehäuse-Management-Netzwerk ein VLAN erstellen.

Für ein VLAN gelten keine besonderen Anforderungen oder Beschränkungen hinsichtlich der IP-Adresse. Der externe Router oder der externe Switch, an den das Onboard Administrator-Modul angeschlossen ist, muss jedoch für den VLAN-Trunk-Modus konfiguriert sein, damit Ethernet-Frames VLAN-Tags für mehrere VLANs an und durch die externe Ethernet-Schnittstelle von Onboard Administrator geleitet werden.

VLAN-Funktionen

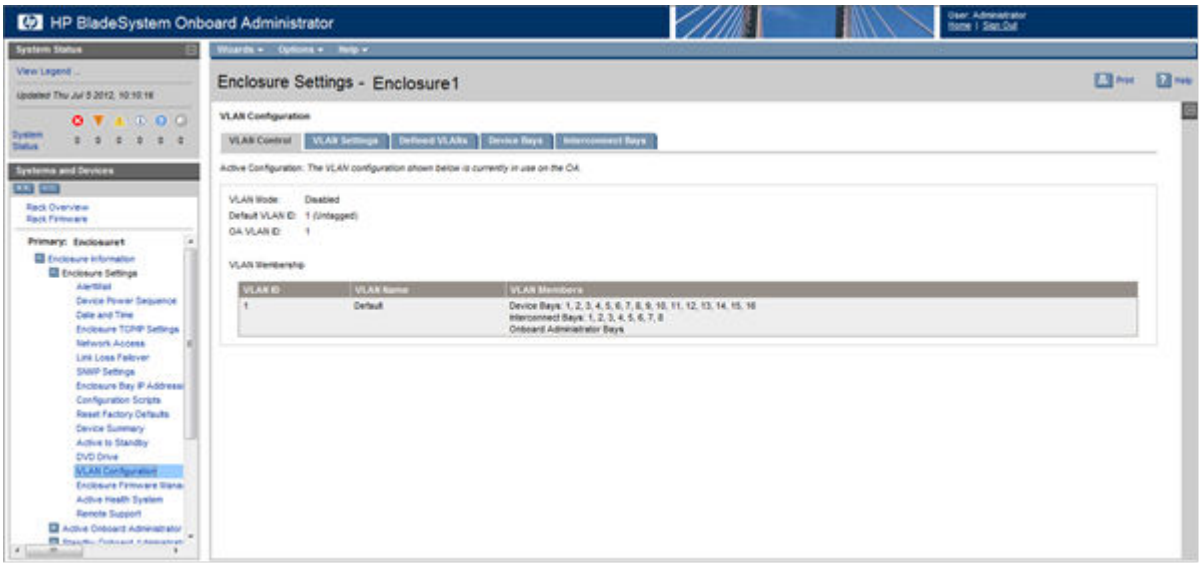
- Die VLAN-ID ist eine eindeutige Nummer, durch die jedes VLAN identifiziert wird. Der zulässige Bereich für VLAN-ID-Nummern ist 1 bis 4094. Standardmäßig ist VLAN deaktiviert, und für alle Geräte ist VLAN ID 1 festgelegt. Nach der Konfiguration eines VLAN können Geräte, die nicht über die gleiche VLAN-ID verfügen, nicht miteinander kommunizieren.
- Alle von Onboard Administrator empfangenen ungetaggten Frames wird die Standard-VLAN-ID zugewiesen. Onboard Administrator sendet als Antwort ungetaggte Frames. Alle getaggten Frames besitzen eine VLAN-ID oder ein VLAN-Tag im Frame, und Onboard Administrator antwortet mit getaggten Frames.
- Wird ein getaggter Frame unter Verwendung der Standard-VLAN-ID gesendet, dann wird er von Onboard Administrator verworfen, da Onboard Administrator erwartet, dass Frames mit der Standard-VLAN-ID ungetaggt sind. Sind Server oder Verbindungsmodule das Ziel, dann antwortet Onboard Administrator mit ungetaggten Frames.
- Da der Datenverkehr zwischen dem iLO/IOM und dem Broadcom-Switch ungetaggt ist, ist das VLAN für sie transparent. Der für das Gerät bestimmte eingehende Datenverkehr wird von Onboard Administrator auf dem Weg zum Broadcom-Switch getaggt, der das Tag dann entfernt, bevor er den Datenverkehr zum Gerät sendet. Der Broadcom-Switch fügt an dem Port, an dem das Gerät angeschlossen ist, die Standard-VLAN-ID zum abgehenden Datenverkehr des Geräts hinzu, bevor er ihn aussendet.
- Die VLAN-ID des Servers, des Verbindungsmoduls und des Onboard Administrator-Moduls ist konfigurierbar. Onboard Administrator kann Teil eines jeden Netzwerks sein, indem seine VLAN-ID so konfiguriert wird, dass sie der Standard-VLAN-Einstellung des externen Switch entspricht, an den das Onboard Administrator-Modul angeschlossen ist.
- Die Onboard Administrator-Firmware weist die Standard-VLAN-ID allen nicht konfigurierten Einschüben zu. Die Standard-VAN-ID kann vom Benutzer geändert werden. Sie können einen auf 31 alphanumerische Zeichen beschränkten Namen mit einer VLAN-ID verknüpfen. Sie können jeweils bis zu 25 VLAN-Einträge mit einer VLAN-ID und einem Namen speichern.
- VLAN unterstützt Peer-to-Peer-Kommunikation zwischen SAS-Verbindungsmodulen. Neben eingeschränkter LCD-Unterstützung werden die CLI- und GUI-Benutzeroberflächen voll unterstützt. Sie können VLAN aktivieren und deaktivieren und VLAN-IDs über das Insight Display anzeigen oder ändern. VLAN wird auf dem Gehäuse-Link und Service-Port nicht unterstützt.
- Für das aktive und für das Onboard Administrator-Standby-Modul werden die gleichen VLAN-Konfigurationseinstellungen festgelegt. Dies bedeutet, dass sich Änderungen am aktiven Onboard Administrator-Modul auch auf das Onboard-Administrator-Standby-Modul auswirken.

Am Onboard-Administrator-Standby-Modul können keine Änderungen vorgenommen, sondern nur die Einstellungen angezeigt werden.

- Sie können VLAN-Einstellungen konfigurieren oder ändern, wenn VLAN deaktiviert ist. Laufzeit-Benutzeränderungen werden nur im RAM gespeichert und gehen verloren, wenn Onboard Administrator neu gestartet wird. Mit dem Befehl `Save Config` (Konfiguration speichern) können Sie Konfigurationsänderungen permanent speichern.
- Sie können VLAN remote konfigurieren. VLAN-Konfigurationsänderungen werden nur im RAM gespeichert, und diese Änderungen werden bei einem Neustart verworfen, sofern sie nicht im FLASH-Speicher gespeichert werden.
- Geräte auf verschiedenen VLAN-Domänennetzwerken können nicht miteinander kommunizieren. Alle Server und Verbindungsmodule können ungeachtet ihrer VLAN-ID weiterhin über das Onboard Administrator-Modul verwaltet werden. Der Client-Computer hat nur Zugriff auf das Onboard Administrator-Modul, wenn für beide die gleiche VLAN-ID festgelegt wurde.

HP empfiehlt, das Netzwerk über ein Konsolenterminal zu konfigurieren, um zu verhindern, dass beim Ändern der VLAN-Konfiguration die Kommunikation verloren geht. Die entsprechenden Änderungen sollten dann auch an der externen Switch vorgenommen werden, an die das Onboard Administrator-Modul angeschlossen ist.

Die Registerkarte „VLAN Control“ (VLAN-Steuerung) zeigt die aktive Konfiguration an, die derzeit auf dem Onboard Administrator verwendet wird.

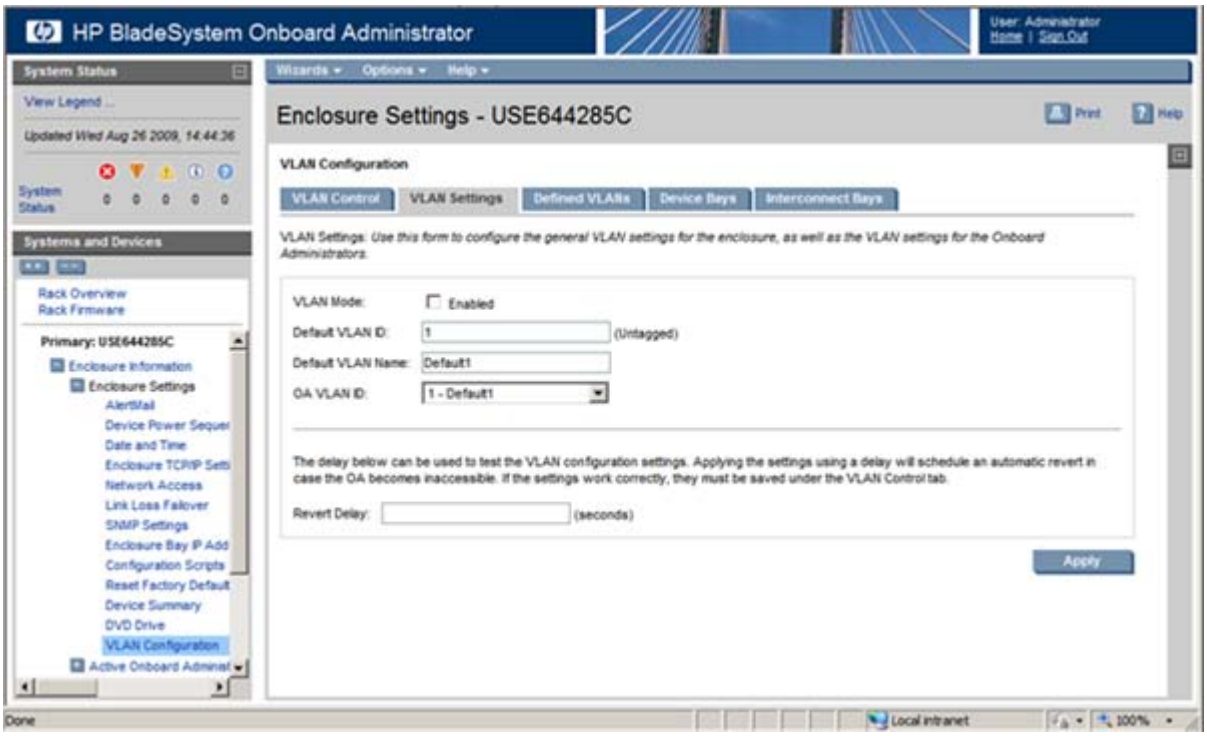


VLAN-Einstellungen

Die allgemeinen VLAN-Einstellungen und die VLAN-Einstellungen für das Onboard Administrator-Modul werden über die Registerkarte „VLAN Settings“ (VLAN-Einstellungen) konfiguriert. Einstellungen für die Komponenten- und Verbindungsmodul-Einschübe werden über die Registerkarten „Device Bays“ (Geräteeinschübe) und „Interconnect Bays“ (Verbindungsmoduleinschübe) konfiguriert. Nachdem Änderungen an diesen drei Registerkarten vorgenommen wurden, wird die Registerkarte „VLAN Control“ (VLAN-Steuerung) angezeigt. Nachdem die Registerkarte „VLAN Control“ (VLAN-Steuerung) angezeigt wurde, können Sie die Einstellungen speichern oder sie auf die vorherigen Einstellungen zurücksetzen.

Die Rücksetzungsverzögerung auf der Registerkarte „VLAN Settings“ (VLAN-Einstellungen) dient zur Planung einer Reversion der Einstellungen auf die Werte, die derzeit auf dem Onboard Administrator-

Modul gespeichert sind. Dies ist hilfreich, sollte die Verbindung bei der Remote-Verwaltung der Einstellungen getrennt werden. Falls Sie die VLAN-Einstellungen falsch konfigurieren und die Verbindung getrennt wird, werden die VLAN-Einstellungen des Onboard Administrator-Moduls auf den vorherigen Zustand vor der Verbindungsherstellung zurückgesetzt.



VLAN Mode (VLAN-Modus) – VLAN ist standardmäßig deaktiviert. Zum Aktivieren der VLAN-Einstellungen aktivieren Sie dieses Kontrollkästchen.

Einstellung	Beschreibung
Default VLAN ID (Standard-VLAN-ID)	Die derzeitige Standard-VLAN-ID-Nummer. Mögliche Werte für die VLAN-ID sind 1 bis 4094.
Default VLAN Name (Standard-VLAN-Name)	Die derzeitige Standard-VLAN-ID-Name. Dieses Feld ist optional und auf maximal 31 Zeichen begrenzt, einschließlich alphanumerischer Zeichen, Bindestriche (-), Unterstriche (_) und Leerstellen.
OA VLAN ID	Die aktuelle OA-VLAN-ID. Um die Mitgliedschaft des Onboard Administrators zu ändern, wählen Sie ein definiertes VLAN aus dem Menü aus. Die Mitgliedschaftsänderung gilt für das aktive und das Onboard Administrator-Standby-Modul.
Revert Delay (Rücksetzungsverzögerung)	Diese Einstellung ermöglicht das automatische Zurücksetzen der VLAN-Konfiguration auf die derzeit gespeicherten Werte, sollte die Verbindung nach Vornahme der VLAN-Konfigurationsänderungen getrennt werden.

Um die Änderungen an der VLAN-Konfiguration vorübergehend zu speichern, klicken Sie auf **Apply** (Übernehmen).

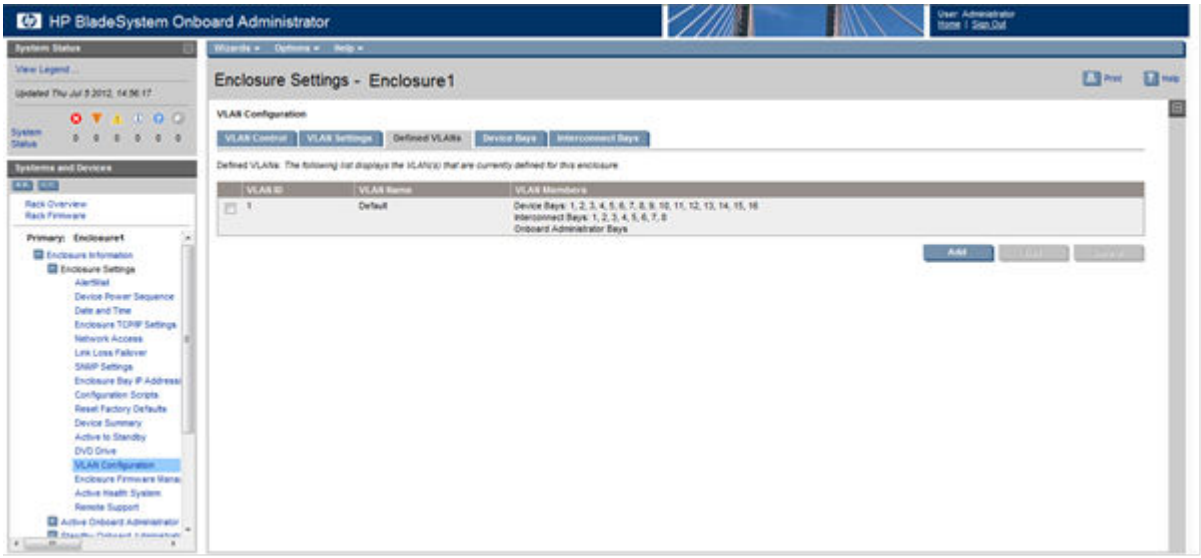
Die Registerkarte „VLAN Control“ (VLAN-Steuerung) wird angezeigt, so dass Sie die Konfigurationsänderungen permanent speichern oder auf die zuvor gespeicherte Konfiguration zurücksetzen können.

HINWEIS: Wenn die Gehäuse-VLAN-Funktion aktiviert ist, vergewissern Sie sich, dass alle HP Virtual Connect Ethernet- und Virtual Connect FC-Verbindungsmodule mit dem gleichen Management-VLAN wie die OA-Module konfiguriert sind. Sorgen Sie bei Virtual Connect-Domänen mit mehreren Gehäusen dafür, dass alle Gehäuse über die gleiche Management-VLAN-Konfiguration für alle VC-Verbindungsmodule und alle OA-Module verfügen.

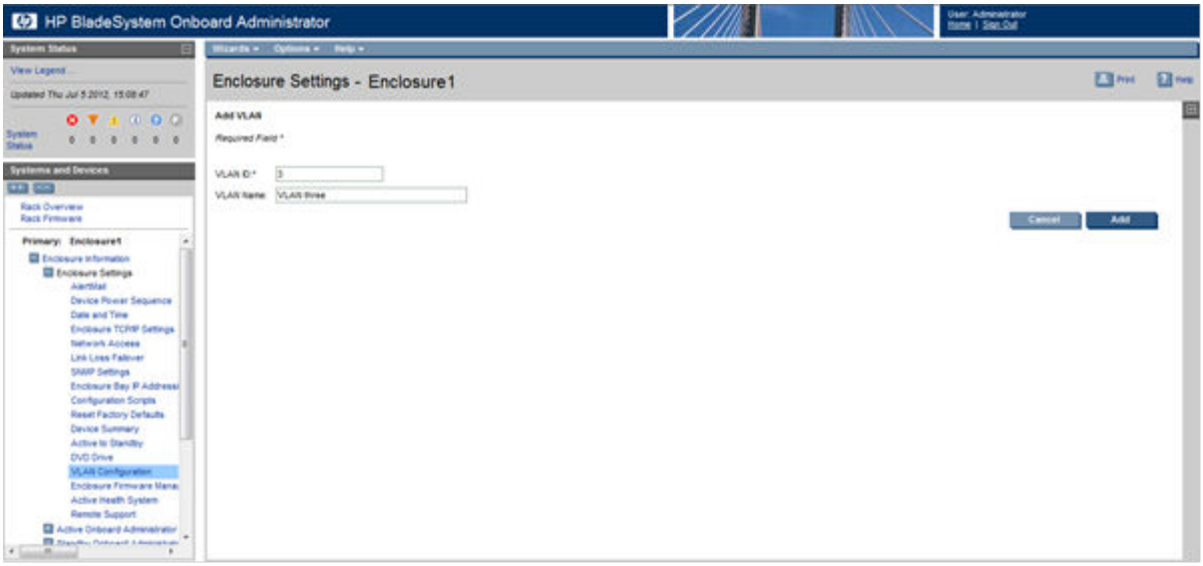
HINWEIS: Wenn die Gehäuse-VLAN-Funktion aktiviert ist, achten Sie darauf, dass alle HP SAS-Switches mit der gleichen Management-VLAN-ID konfiguriert sind wie die OA-Module im betreffenden Gehäuse.

Hinzufügen, Bearbeiten und Entfernen von VLANs

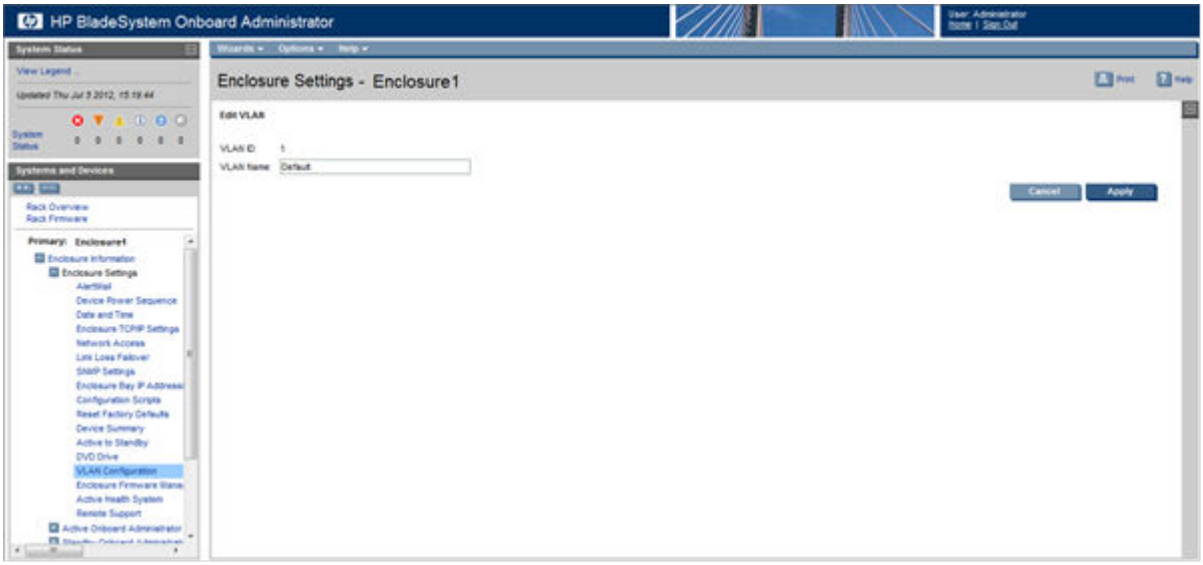
Um ein neues VLAN hinzuzufügen, klicken Sie auf die Registerkarte **Defined VLANs** (Definierte VLANs), und klicken Sie dann auf **Add** (Hinzufügen).



Die Seite „Add VLAN“ (VLAN hinzufügen) wird mit zwei Feldern angezeigt: „VLAN ID“ (VLAN-ID) und „VLAN Name“ (VLAN-Name). Das Feld „VLAN Name“ ist optional. Die VLAN-ID muss eine ganze Zahl zwischen 1 und 4094 sein. Wenn Sie versuchen, ein neues VLAN hinzuzufügen, dessen Name oder ID dem Namen oder der ID eines vorhandenen VLAN entsprechen, wird Ihnen eine Fehlermeldung angezeigt.



Der Name eines bestehenden VLAN kann durch Wechseln zur Registerkarte **Defined VLANs** (Definierte VLANs) bearbeitet werden. Wählen Sie ein VLAN aus, und klicken Sie dann auf **Edit** (Bearbeiten). Die Seite „Edit VLAN“ (VLAN bearbeiten) wird mit einem Feld zum Bearbeiten des VLAN-Namens angezeigt. Der VLAN-Name ist kein erforderliches Feld.



Bestehende VLANs können von der Seite „Defined VLANs“ (Definierte VLANs) entfernt werden. Wählen Sie dazu die betreffenden VLANs aus, und klicken Sie dann auf **Delete** (Löschen). Beim Löschen eines VLAN werden alle seine Mitglieder in das Standard-VLAN verschoben. Das Standard-VLAN kann nicht gelöscht werden.

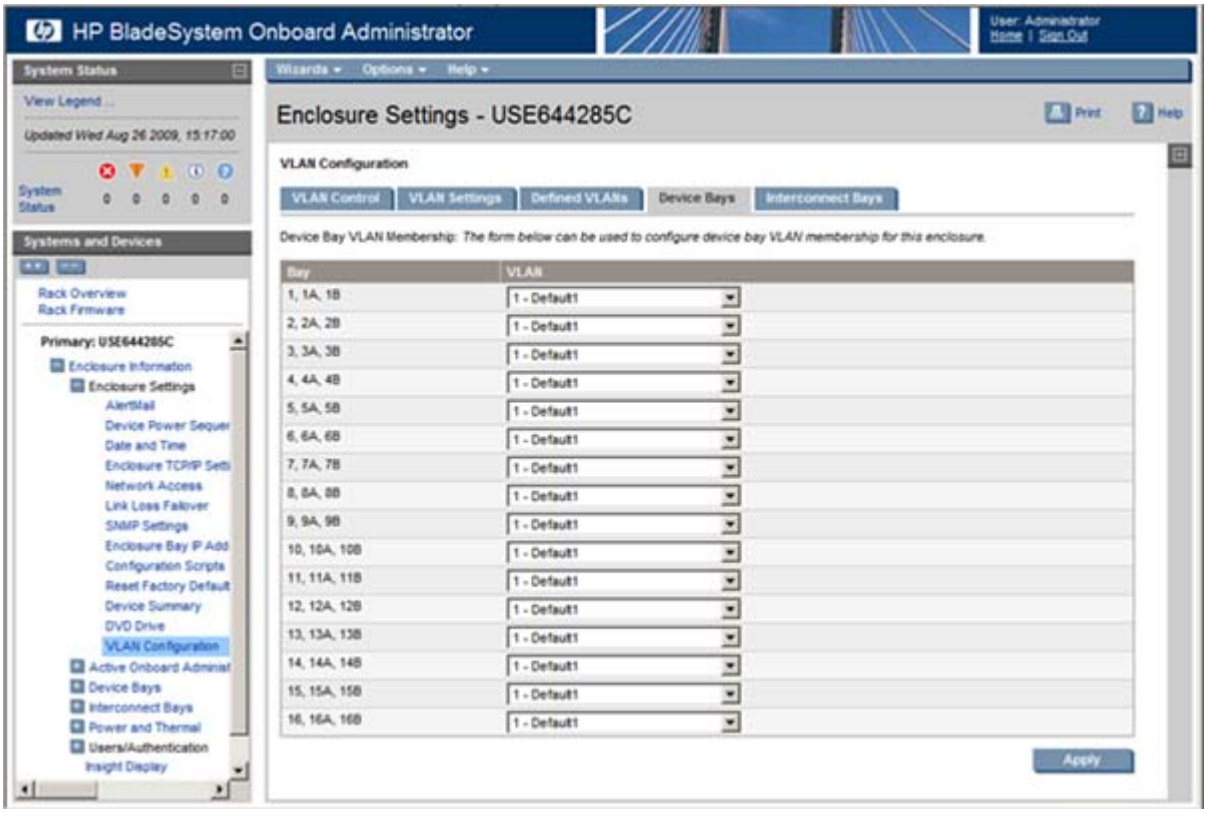
HINWEIS: Der Zugriff auf das aktive OA-Modul über eine verbindungslokale IPv6-Adresse funktioniert möglicherweise nicht auf allen Client-System-Setups, die mehrere Netzwerkschnittstellen beinhalten.

Konfigurieren von Geräten

Nachdem VLANs unter der Registerkarte „Defined VLANs“ (Definierte VLANs) definiert wurden, können Geräte für deren Verwendung zugewiesen werden. Onboard Administrator wird einem VLAN unter der Registerkarte „VLAN Settings“ (VLAN-Einstellungen) zugewiesen. Geräteeinschübe und Verbindungsmoduleinschübe werden unter der Registerkarte „Device Bays“ (Geräteeinschübe) und der Registerkarte „Interconnect Bays“ (Verbindungsmoduleinschübe) zugewiesen.

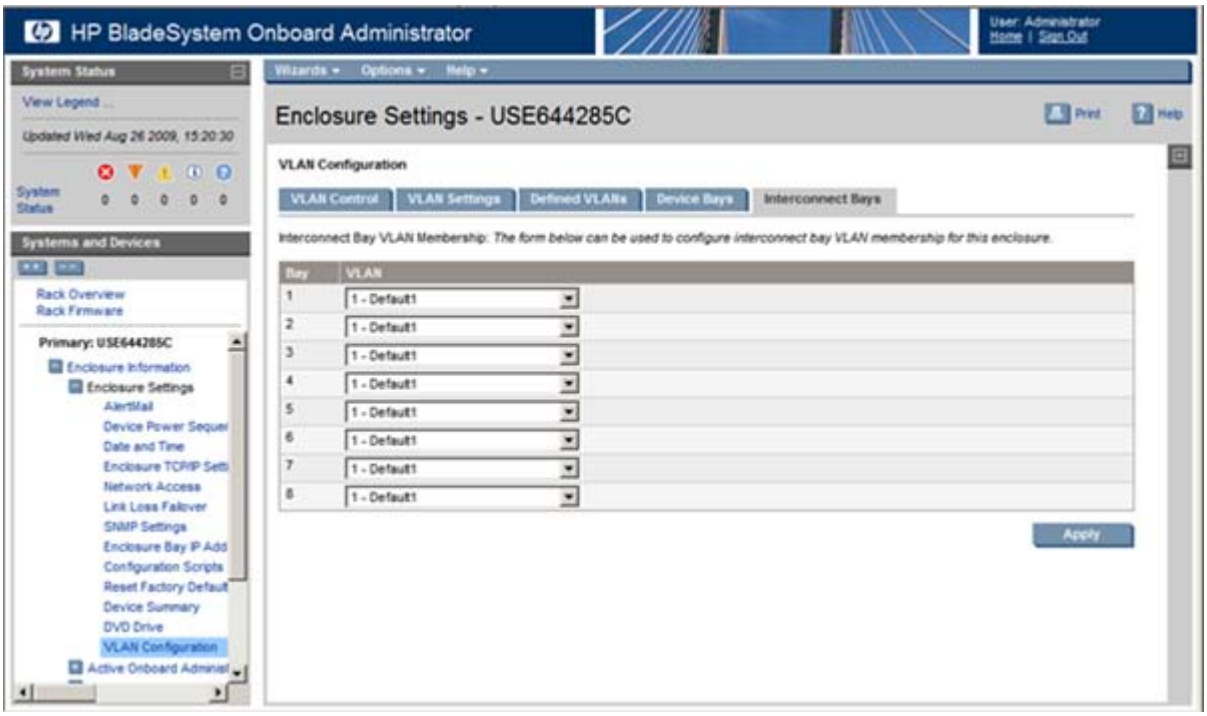
Geräteeinschübe

Um die Mitgliedschaft eines Komponenteneinschubs zu ändern, wählen Sie ein definiertes VLAN aus dem Menü unter der VLAN-Spalte aus, und klicken Sie auf **Apply** (Übernehmen).

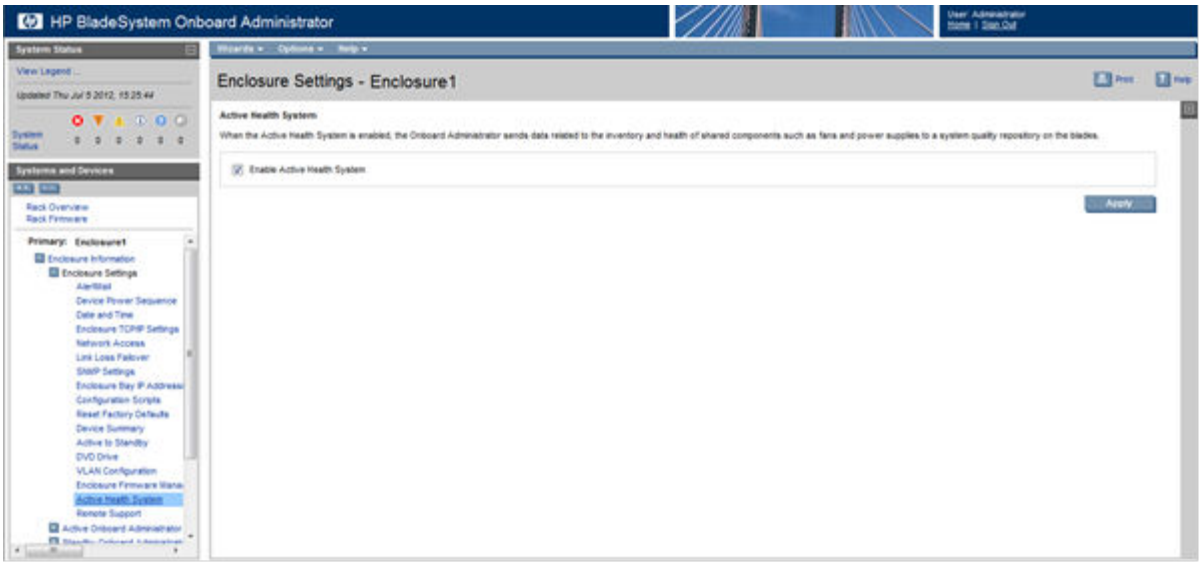


Verbindungsmoduleinschübe

Um die Mitgliedschaft eines Verbindungsmoduleinschubs zu ändern, wählen Sie ein definiertes VLAN aus dem Menü unter der VLAN-Spalte aus, und klicken Sie auf **Apply** (Übernehmen).



Active Health System



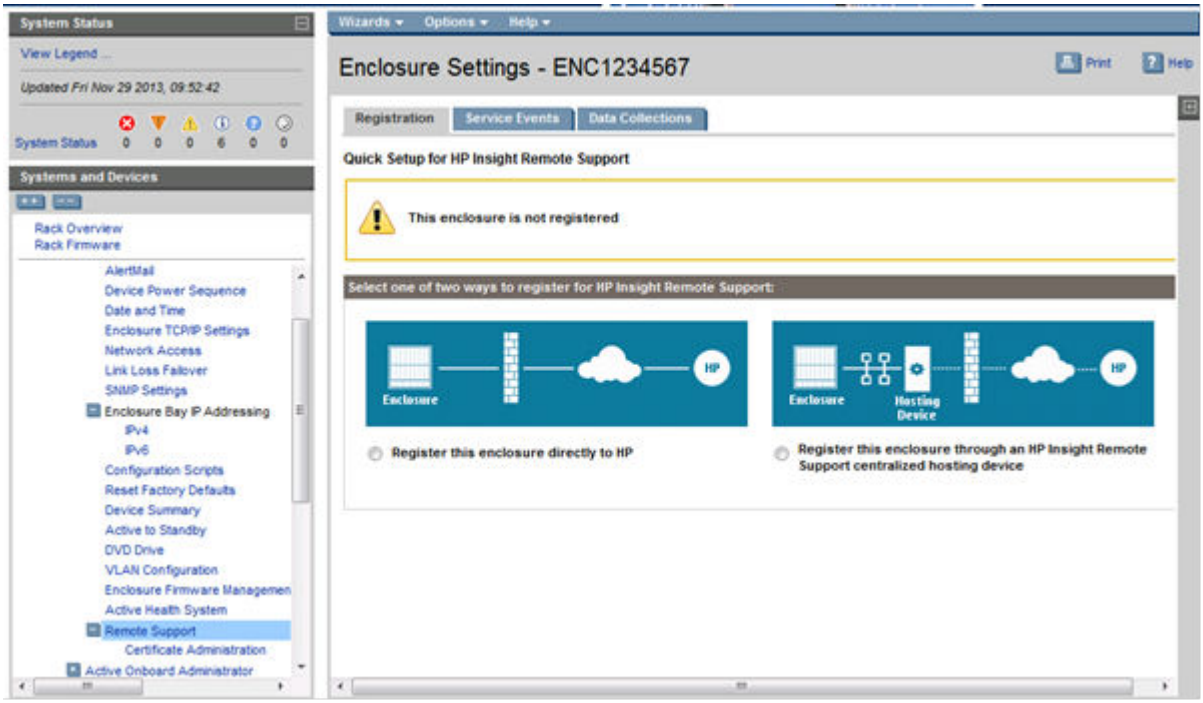
Das HP Active Health System überwacht und verzeichnet Änderungen an der Serverhardware und der Systemkonfiguration Das Active Health System erleichtert die Diagnose von Problemen und die Bereitstellung einer schnellen Lösung bei Systemfehlern. In einem HP BladeSystem Gehäuse stellt Onboard Administrator Daten bezüglich gemeinsam genutzter Infrastrukturkomponenten und Systemeinstellungen für das auf den HP ProLiant Server Blades befindliche Active Health System bereit. HP Active Health System erfasst keine Informationen zu Active Health System-Benutzervorgängen, Finanzen, Kunden, Mitarbeitern, Partnern oder Rechenzentren (wie z. B. IP-Adressen, Hostnamen, Benutzernamen und Kennwörter). Beispiele für durch Onboard Administrator erfasste Daten sind Bestands- und Statusinformationen für die folgenden Komponenten und Einstellungen:

- Gehäuselüfter
- Gehäuse-Netzteile
- Verbindungsmodule
- Gehäuse-Midplane
- Onboard Administrators

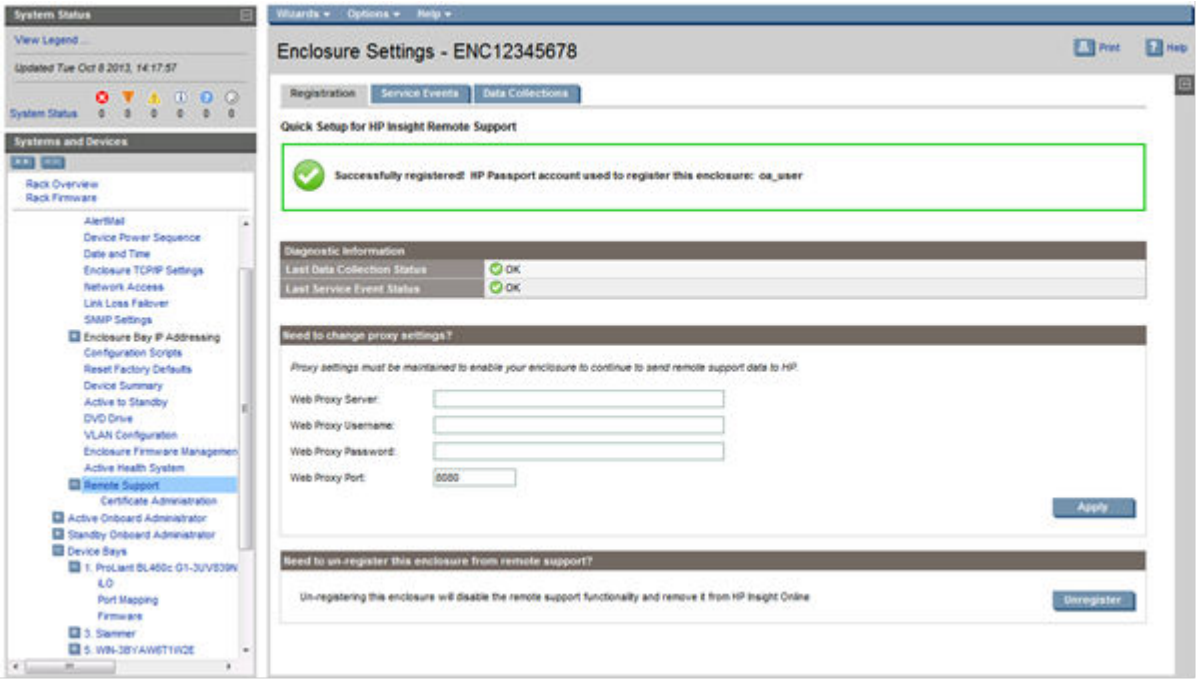
Gehäuse-Strommessungen

Insight Remote Support-Registrierung

Der folgende Bildschirm zeigt die Registrierungsregisterkarte von Remote Support mit dem noch nicht registrierten Gehäuse an:



Der folgende Bildschirm zeigt die Registrierungsregisterkarte von Remote Support mit dem registrierten Gehäuse an:


System Status
View Legend ...
Updated Tue Oct 8 2013, 14:17:57
System Status
Systems and Devices
Rack Overview
Rack Firmware
Enclosure Settings - ENC12345678
Print
Help
Registration
Service Events
Data Collections
Quick Setup for HP Insight Remote Support
Successfully registered! HP Passport account used to register this enclosure: oa_user
Diagnostic Information
Last Data Collection Status
OK
Last Service Event Status
OK
Need to change proxy settings?
Proxy settings must be maintained to enable your enclosure to continue to send remote support data to HP.
Web Proxy Server:
Web Proxy Username:
Web Proxy Password:
Web Proxy Port:
8080
Apply
Need to un-register this enclosure from remote support?
Un-registering this enclosure will disable the remote support functionality and remove it from HP Insight Online
Unregister

HP hat eine Service- und Supportlösung geschaffen, durch die viele tägliche Aufgaben automatisiert und Risiken reduziert werden. HP integriert ein personalisiertes Online-Dashboard (HP Insight Online), ein Support-Portal und eine mobile App (HP Support Center) sowie Remote-Support rund um die Uhr (HP Insight Remote Support) für die konsolidierte Infrastruktur.

Wenn Sie die integrierte Remote Support-Funktionalität mit einem HP BladeSystem c-Class-Gehäuse verwenden, können Sie aus folgenden Konfigurationsoptionen wählen:

- **Insight Online Direct Connect** (Insight Online-Direktverbindung): Registrieren Sie ein Gehäuse für die direkte Kommunikation mit HP Insight Online, ohne ein zentrales HP Insight Remote Support-Hostinggerät in der lokalen Umgebung konfigurieren zu müssen. HP Insight Online dient als Hauptbenutzeroberfläche für Remote Support-Informationen. Die Direktverbindungskonfiguration ist in Onboard Administrator 4.11 und höher verfügbar.
- **Insight Remote Support Central Connect** (Insight Remote Support-Zentralverbindung): Registrieren Sie ein Gehäuse für die Kommunikation mit HP über ein zentrales HP Insight Remote Support-Hostinggerät in der lokalen Umgebung. Alle Konfigurations- und Serviceereignisinformationen werden über das Hostinggerät geleitet. Diese Informationen können über die lokale HP Insight RS Console oder die webbasierte Ansicht in HP Insight Online angezeigt werden. Die Zentralverbindungskonfiguration ist auf Onboard Administrator 3.60 und höher verfügbar.

Durch Insight Remote Support gesammelte Daten

Wenn das BladeSystem-Gehäuse bei Insight Remote Support registriert wird, werden die folgenden Informationen zu gemeinsam genutzten Infrastrukturkomponenten des BladeSystem-Gehäuses innerhalb des Gehäuses zu HP gesendet:

- Registrierung: Im Rahmen des Gehäuse-Registrierungsvorgangs sendet Onboard Administrator bei der Zentralverbindung die Daten zum Insight Remote Support-Hostingserver, durch die die Gehäusehardware eindeutig identifiziert wird. Bei einer Direktverbindung sendet Onboard Administrator die Daten direkt an einen Webdienst im Remote Support Data Center.

  Beispiele der erfassten Daten umfassen:

  - Gehäusename
  - Gehäuse-Produktname
  - Gehäuseteilenummer
  - Gehäuse-Seriennummer
  - Name des Gehäuseherstellers
  - Onboard Administrator-Firmwareversion
  - Onboard Administrator-IP- und MAC-Adressen
- Service-Ereignisse – Als Teil des Service-Ereignisvorgangs sendet Onboard Administrator Daten, um die relevante Hardwarekomponente dem Insight Remote Support-Hostgerät gegenüber eindeutig zu identifizieren.

  Beispiele der erfassten Daten umfassen:

  - Gehäusemodell
  - Gehäuse-Seriennummer
  - Teilenummer der relevanten Hardwarekomponente
  - Beschreibung, Position und andere identifizierende Merkmale der relevanten Hardwarekomponente

  Weitere Informationen finden Sie unter „Insight Remote Support-Serviceereignisse“ (Insight Remote Support-Serviceereignisse auf Seite 192).
- Datensammlungen – Als Teil des Datenerfassungsvorgangs sendet der Onboard Administrator Daten zu Insight Remote Support, um eine proaktive Empfehlung und Beratung zu ermöglichen. Es werden Informationen bezüglich der Gehäuse-Hardware sowie bestückter

Systemkomponenten gesendet, darunter LCD-Modul, Onboard Administrator-Module, Gehäuse-Lüftermodule, Gehäuse-Netzteilmodule, Verbindungsmodule und Server Blades.

Es folgen Beispiele der für diese Systemkomponenten erfassten Daten:

- Hardware-Modulbeschreibungen wie Hersteller, Produktname, Seriennummer, UUID, Teilenummer und Position innerhalb des Gehäuses
- Firmware-Revision
- Diagnose- und Statusinformationen
- Strom- und thermische Konfigurations- und Statusinformationen
- Netzwerk- und Anschlussbelegungs-Informationen

Weitere Informationen finden Sie unter „Insight Remote Support-Datensammlungen“ (Insight Remote Support-Datensammlungen auf Seite 193).

Voraussetzungen

Bevor Sie sich registrieren, überprüfen Sie, ob die folgenden Voraussetzungen erfüllt sind:

- Auf allen OA-Modulen im Gehäuse wird eine unterstützte Version der OA-Firmware installiert.
  - Für die Registrierung für die Insight Remote Support-Zentralverbindung ist Version 3.60 oder höher erforderlich.
  - Für die Registrierung für die Insight Online-Direktverbindung ist Version 4.11 oder höher erforderlich.

  Die jeweils aktuelle Version können Sie von der HP Website (http://www.hp.com/go/oa) herunterladen.
- Nur für die Insight Online-Direktverbindung: In Onboard Administrator ist ein DNS-Server konfiguriert. Dies ist für die Kommunikation zwischen iLO und Insight Online erforderlich.
- Nur für die Remote Support-Zentralverbindung: Insight RS Version 7.0.5 oder höher ist auf dem Insight RS-Hostinggerät installiert und konfiguriert.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, ist beim Anschluss an ein HP Insight Remote Support-Hostinggerät ein gültiges Zertifikat erforderlich.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

Registrieren für Insight Remote Support über die OA-Weboberfläche

HP Insight Remote Support sendet Hardware-Ereignisse automatisch an HP, um Ausfallzeiten zu vermeiden und eine schnellere Problembehebung zu ermöglichen. Sie können sich direkt oder über ein Insight RS Hostinggerät bei HP registrieren.

Registrieren für Insight Remote Support über eine Direktverbindung

Verfahren Sie zum Registrieren eines HP BladeSystem c-Class-Gehäuses für eine Insight Online-Direktverbindung wie folgt. Bei einer Registrierung für die Insight Online-Direktverbindung müssen die Schritte auf der OA-Benutzeroberfläche und im Insight Online-Portal durchgeführt werden.

1. Stellen Sie sicher, dass das System die Voraussetzungen für die Verwendung der Insight Remote Support-Lösung erfüllt. Weitere Informationen hierzu finden Sie im Abschnitt „Voraussetzungen“.
2. Navigieren Sie zur Seite **Enclosure Information (Gehäuseinformationen)>Enclosure Settings (Gehäuseeinstellungen)>Remote Support**.
3. Wählen Sie auf der Registerkarte **Registration** (Registrierung) die Option **Register this enclosure directly to HP** (Dieses Gehäuse direkt bei HP registrieren). Die Seite wird mit den Direktverbindungs-Registrierungsoptionen aktualisiert.
4. Geben Sie in die Felder **HP Passport User ID** (HP Passport-Benutzer-ID) und **HP Passport Password** (HP Passport-Kennwort) Ihre HP Passport-Anmeldeinformationen ein.

HINWEIS: Geben Sie in das Feld **HP Passport User ID** (HP Passport-Benutzer-ID) Ihre HP Passport-Benutzer-ID ein. In den meisten Fällen ist die HP Passport Benutzer-ID die bei der Registrierung für HP Passport angegebene E-Mail-Adresse. Wenn Sie die Benutzer-ID in HPSC geändert haben, geben Sie die Benutzer-ID anstelle der E-Mail-Adresse ein.

5. Optional: Wenn Ihr HP BladeSystem c-Class-Gehäuse über einen Webproxyserver auf das Internet zugreift, machen Sie die folgenden Angaben:
   - **Web Proxy Server (Webproxyserver)**
   - **Web Proxy Username (Webproxybenutzername)**
   - **Web Proxy Password (Webproxykennwort)**
   - **Web Proxy Port (Webproxyanschluss)**
6. Aktivieren Sie das Kontrollkästchen **I accept the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization** (Ich stimme den Bedingungen des HP Softwarelizenzvertrags und der zusätzlichen Lizenzautorisierung für HP Insight Management zu). Diese Dokumente können auf der Website für HP Softwarelizenzdokumente (http://www.hp.com/go/SWLicensing) eingesehen werden.
7. Klicken Sie auf **Register** (Registrieren). Das Klicken auf **Register** (Registrieren) ist der erste Schritt des aus zwei Schritten bestehenden Registrierungsvorgangs. Schritt 2 wird in HP Insight Online durchgeführt.

   Durch die Registrierung stimmen Sie zu, Daten zur Registrierung, zu Serviceereignissen und zur Konfiguration an HP zu senden. Alle erfassten und an HP gesendeten Daten werden gemäß der HP Datenschutzrichtlinie gehandhabt. Sie können die HP Datenschutzrichtlinie auf der HP Website (http://www.hp.com/go/privacy) einsehen.

   Wenn Schritt 1 des Registrierungsvorgangs beginnt, erscheint die folgende Meldung:

   ```
   Step 1 of registration in progress, please wait...
   ```

   Wenn Schritt 1 abgeschlossen ist, erscheint die folgende Meldung:

   ```
   Step 1 of remote support registration has been completed. Please
   proceed to step 2 to complete the registration process.
   ```

   Es kann bis zu fünf Minuten dauern, bis die Registrierungsanforderung verarbeitet wurde.
8. Navigieren Sie zur HP Insight Online-Website (http://www.hp.com/go/insightonline.), und melden Sie sich mit den Anmeldeinformationen Ihres HP Passport-Kontos an.
9. Befolgen Sie die Anweisungen auf dem Bildschirm in Insight Online, und geben Sie Ihren Standort sowie Kontakt- und Partnerinformationen an, so dass HP den Service für Ihr Gehäuse zustellen kann. Ausführliche Informationen finden Sie im *HP Insight Remote Support and Insight*

Online Setup Guide for HP ProLiant Servers and HP BladeSystem c-Class Enclosures (HP Insight Remote Support und Insight Online Konfigurationshandbuch für HP ProLiant Server und HP BladeSystem c-Class Gehäuse).

10. Kehren Sie zur Seite **Remote Support** auf der OA-Weboberfläche zurück, aktivieren Sie das Kontrollkästchen **Please confirm that you have completed the registration process in HP Insight Online** (Bitte bestätigen, dass der Registrierungsvorgang in HP Insight Online durchgeführt wurde), und klicken Sie dann auf **Apply** (Übernehmen).

    Die folgende Meldung erscheint:

    ```
    Are you sure you have completed registration in HP Insight Online?
    Click OK to confirm or Cancel to cancel.
    ```

11. Klicken Sie auf **OK**. Es wird eine Meldung angezeigt, die der Folgenden ähnelt:

    ```
    Successfully registered!

    HP Passport User ID used to register this enclosure: <HP Passport-
    Benutzer-ID>.
    ```

12. Optional: Senden Sie ein Testereignis, um die Verbindung zwischen OA und Insight Remote Support zu bestätigen.

    a. Öffnen Sie **Enclosure Settings (Gehäuseeinstellungen)>Remote Support**.

    b. Klicken Sie auf die Registerkarte **Service Events** (Dienstereignisse) (Insight Remote Support-Serviceereignisse auf Seite 192) (Insight Remote Support-Serviceereignisse auf Seite 192).

    c. Klicken Sie auf **Send Test Event** (Testereignis senden)

13. Optional: Um E-Mail-Benachrichtigungen zu Systemereignissen zu erhalten, konfigurieren Sie AlertMail auf der Seite **Enclosure Information (Gehäuseinformationen)>Enclosure Settings (Gehäuseeinstellungen)>AlertMail** (AlertMail auf Seite 116) (AlertMail auf Seite 116).

Bearbeiten der Webproxy-Einstellungen

Proxyeinstellungen müssen verwaltet werden, damit Ihr Gehäuse fortgesetzt Remote Support-Daten an HP senden kann. Sollten sich die Proxy-Einstellungen ändern, können Sie sie mit dem folgenden Verfahren bearbeiten:

1. Navigieren Sie zur Seite **Enclosure Information>Enclosure Settings>Remote Support** (Gehäuseinformationen>Gehäuseeinstellungen>Remote Support).
2. Aktualisieren Sie bei Bedarf die folgenden Einstellungen:
    - **Web Proxy Server** (Webproxyserver): Geben Sie den Webproxyserver im Format http://<Hostname oder IP-Adresse> ein.
    - **Web Proxy Port (Webproxyanschluss)**
    - **Web Proxy Username (Webproxybenutzername)**
    - **Web Proxy Password (Webproxykennwort)**
3. Klicken Sie auf **Apply** (Übernehmen).

Registrieren für Insight Remote Support über eine Zentralverbindung

Verfahren Sie zum Registrieren eines HP BladeSystem c-Class-Gehäuses für eine Insight Remote Support-Zentralverbindung wie folgt:

1. Stellen Sie sicher, dass das System die Voraussetzungen für die Verwendung von Insight Remote Support erfüllt. Weitere Informationen hierzu finden Sie im Abschnitt „Voraussetzungen“.
2. Navigieren Sie zur Seite **Enclosure Information (Gehäuseinformationen)>Enclosure Settings (Gehäuseeinstellungen)** (Network Access (Netzwerkzugriff) auf Seite 136) (Network Access (Netzwerkzugriff) auf Seite 136), und klicken Sie auf die Registerkarte **Protocol** (Protokoll).
3. Vergewissern Sie sich, dass das Kontrollkästchen „Enable XML Reply“ (XML-Antwort aktivieren) aktiviert ist.

   Wenn dieses Kontrollkästchen nicht aktiviert ist, kann das Insight RS-Hostinggerät keine Daten von dem Onboard Administrator erfassen.
4. Navigieren Sie zur Seite **Enclosure Information (Gehäuseinformationen)>Enclosure Settings (Gehäuseeinstellungen)>Remote Support**.
5. Wählen Sie **Register this enclosure through an HP Insight Remote Support centralized hosting device** (Dieses Gehäuse über ein zentralisiertes HP Insight Remote Support-Hosting-Gerät registrieren) aus. Die Seite wird aktualisiert, um die Optionen für die zentrale Registrierung anzuzeigen.
6. Geben Sie den Hostnamen des Insight RS-Hostinggeräts oder die IP-Adresse und Portnummer ein. Der Standard-Port ist 7906.
7. Klicken Sie auf **Register** (Registrieren). Durch die Registrierung stimmen Sie zu, Daten zur Registrierung, zu Serviceereignissen und zur Konfiguration an HP zu senden. Alle gesammelten und an HP gesendeten Daten werden gemäß der HP Datenschutzerklärung behandelt. Sie können die HP Datenschutzrichtlinie auf der HP Website (http://www.hp.com/go/privacy) einsehen. Die folgende Meldung wird angezeigt:

   ```
   Device successfully registered.
   ```
8. Optional: Senden Sie ein Testereignis, um die Verbindung zwischen OA und Insight Remote Support zu bestätigen.
   a. Gehen Sie zu **Enclosure Settings > Remote Support** (Gehäuseeinstellungen > Remote Support).
   b. Klicken Sie auf die Registerkarte **Service Events** (Dienstereignisse) (Insight Remote Support-Serviceereignisse auf Seite 192).
   c. Klicken Sie auf **Send Test Event** (Testereignis senden)

Aufheben der Registrierung eines HP BladeSystem c-Class-Gehäuses für eine Insight Online-Direktverbindung

1. Navigieren Sie zur Seite **Enclosure Information>Enclosure Settings>Remote Support** (Gehäuseinformationen>Gehäuseeinstellungen>Remote Support).
2. Klicken Sie auf **Unregister** (Registrierung aufheben).

   Die folgende Meldung wird angezeigt: `Are you sure you want to un-register and disable HP Insight Remote Support?`
3. Klicken Sie auf **OK**.

   Die folgende Meldung wird angezeigt: `Un-registration in progress Please wait…`

   Nachdem die Registrierung aufgehoben wurde, wird auf der Remote Support-Seite die folgende Meldung angezeigt:

   ```
   The enclosure is not registered.
   ```

Aufheben der Registrierung eines HP BladeSystem c-Class-Gehäuses für eine Central Connect Remote Support-Zentralverbindung

1. Melden Sie sich bei der Insight RS Console an.
2. Führen Sie einen der folgenden Schritte durch:
   - Um die Überwachung eines HP BladeSystem c-Class Gehäuses vorübergehend auszusetzen, wählen Sie den Server auf der Registerkarte **Devices>Device Summary** (Geräte>Gerätezusammenfassung) in der HP Insight RS Console aus. Wählen Sie dann **ACTIONS>DISABLE SELECTED** (AKTIONEN>AUSGEWÄHLTE DEAKTIVIEREN).
   - Um die Überwachung eines HP BladeSystem c-Class Gehäuses permanent zu stoppen, löschen Sie das Gehäuse aus der Insight RS Console. Um das Gehäuse zu löschen, wählen Sie es auf der Registerkarte **Device Summary** (Gerätezusammenfassung) aus, und wählen Sie dann **ACTIONS>DELETE SELECTED** (AKTIONEN>AUSGEWÄHLTE LÖSCHEN).

   Durch die Deaktivierung oder das Löschen des Gehäuses in der Insight RS Console wird die Registrierung des Geräts in OA nicht aufgehoben. Damit Onboard Administrator erkennt, dass ein Gehäuse deaktiviert wurde, müssen Sie die Registrierung bei Insight Remote Support über Onboard Administrator durchführen.
3. Navigieren Sie zur Seite **Enclosure Information>Enclosure Settings>Remote Support** (Gehäuseinformationen>Gehäuseeinstellungen>Remote Support) auf der OA-Weboberfläche.
4. Klicken Sie auf **Unregister** (Registrierung aufheben).

   Die folgende Meldung wird angezeigt: `Are you sure you want to un-register and disable HP Insight Remote Support?`
5. Klicken Sie auf **OK**.

   Die folgende Meldung wird angezeigt: `The enclosure is not registered.`

Verbindungsfehler während der Registrierung für eine OA-Direktverbindung

Problem: Der folgende Fehler tritt bei dem Versuch auf, ein HP BladeSystem c-Class Gehäuse für eine Insight Online-Direktverbindung zu registrieren:

```
Failed to resolve HP Insight Remote Support direct connect web service.
Please verify DNS settings, proxy settings and connectivity.
```

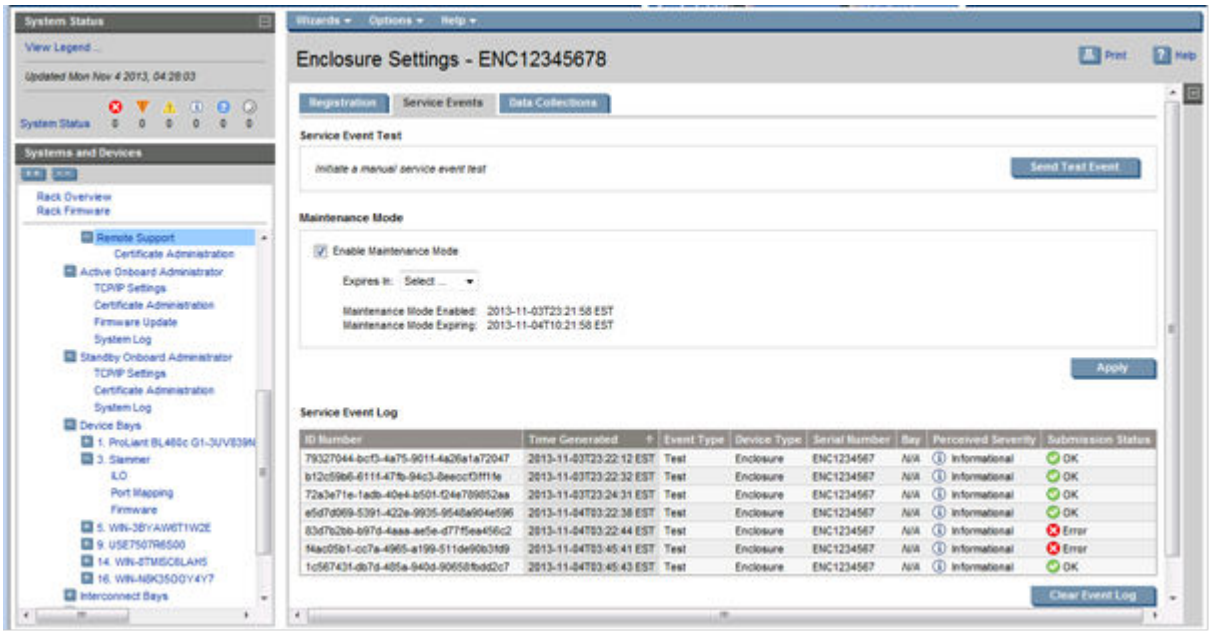
Lösung 1: Stellen Sie sicher, dass die DNS-Einstellungen im OA korrekt konfiguriert sind. Sie können diese Aufgabe über die OA-Weboberfläche oder CLI ausführen:

- Melden Sie sich bei der OA-Weboberfläche an und navigieren Sie zur Seite **Active Onboard Administrator (Aktiver Onboard Administrator)>TCP/IP Settings (TCP/IP-Einstellungen)** (Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator auf Seite 212). Überprüfen Sie, ob die DNS-Konfiguration richtig ist Klicken Sie zum Bearbeiten der Konfiguration auf den folgenden Link unten auf dem Bildschirm: **Click here to modify the TCP/IP settings.** (Hier klicken, um die TCP/IP-Einstellungen zu ändern).
- Melden Sie sich bei der OA CLI-Schnittstelle an, und führen Sie den Befehl `SHOW NETWORK` aus. Überprüfen Sie, ob die DNS-Konfiguration richtig ist Verwenden Sie zum Bearbeiten der Konfiguration den Befehl `ADD OA DNS`.

Lösung 2: Stellen Sie sicher, dass die Webproxy-Einstellungen im OA korrekt konfiguriert sind.

Lösung 3: Stellen Sie sicher, dass Ihre Konfiguration den Netzwerkanforderungen für eine Insight Online-Direktverbindung entspricht.

Insight Remote Support-Serviceereignisse



Über die Seite „Remote Support Service Events“ (Remote Support-Serviceereignisse) können Sie Serviceereignisse überwachen, Testereignisse senden oder den Wartungsmodus festlegen.

Ein Serviceereignis ist ein Hardwarefehler, wie z. B. ein Problem mit einem Netzteilmodul oder einem Lüftermodul eines Gehäuses. Wenn das BladeSystem-Gehäuse mit Insight Remote Support registriert ist, werden Serviceereignisse protokolliert und zu HP gesendet. Wenn HP ein Serviceereignis empfängt, wird ein Supportfall geöffnet und im Serviceereignis-Protokoll werden Details angezeigt.

HINWEIS: Um E-Mail-Benachrichtigungen zu Systemereignissen zu erhalten, konfigurieren Sie AlertMail auf der Seite **Enclosure Information>Enclosure Settings>AlertMail** (Gehäuseinformationen>Gehäuseeinstellungen>AlertMail).

Verwenden des Wartungsmodus

Im Wartungsmodus kann ein System gewartet werden. Wenn in dieser Zeit ein Serviceereignis generiert wird, gibt es an, dass sich das System im Wartungsmodus befindet. Mittels dieses Serviceereignisses kann HP bestimmen, ob ein Servicefall geöffnet werden muss. Wenn der Wartungsmodus zu diesem Zeitpunkt nicht ausdrücklich vom Benutzer ausgeschaltet wird, wird er nach Ablauf der ausgewählten Zeitspanne automatisch von Onboard Administrator ausgeschaltet.

So verwenden Sie den Wartungsmodus:

1. Aktivieren Sie das Kontrollkästchen **Enable Maintenance Mode** (Wartungsmodus aktivieren).
2. Wählen Sie im Menü **Expires in** (Läuft ab in) eine Zeitspanne aus.
3. Klicken Sie auf **Apply** (Übernehmen).

Der Wartungsmodus wird nach Ablauf der ausgewählten Zeitspanne automatisch beendet.

TIPP: Wenn der Wartungsmodus frühzeitig beendet werden soll, deaktivieren Sie das Kontrollkästchen **Enable Maintenance Mode** (Wartungsmodus aktivieren) und klicken Sie dann auf **Apply** (Übernehmen).

Senden eines Service-Testereignisses

Um sicherzustellen, dass Ihre Insight Remote Support-Konfiguration korrekt ist, klicken Sie auf **Send Test Event** (Testereignis senden), um ein Testereignis zu senden.

Wenn die Übertragung abgeschlossen ist, wird das Testereignis im Serviceereignis-Protokoll aufgelistet.

Anzeigen des Serviceereignis-Protokolls

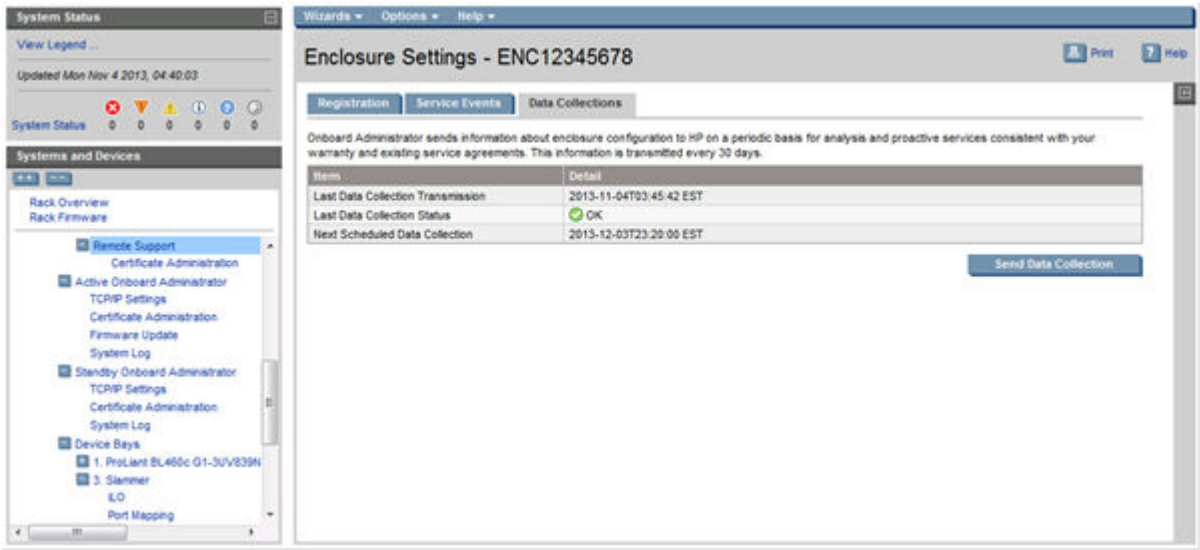
Im Serviceereignis-Protokoll werden die folgenden Details zu jedem Serviceereignis angezeigt:

Zeile	Beschreibung
ID Number (LUN-Nummer)	Eine eindeutige Zeichenfolge, anhand der das Serviceereignis identifiziert wird.
Time Generated (Erstellungszeitpunkt)	Der Zeitpunkt, an dem das Serviceereignis generiert wurde
Event Type (Ereignistyp)	Jedes Ereignis ist als vom Typ „System“ oder „Test“ klassifiziert
Device Type (Gerätetyp)	Eine Zeichenfolge, anhand der die Quelle des Ereignisses identifiziert wird. Mögliche Werte sind: Fan (Lüfter), Power Supply (Netzteil), Onboard Administrator, Interconnect (Verbindungsmodul), Enclosure (Gehäuse).
Serial Number (Seriennummer)	Eine Zeichenfolge, die die Seriennummer des Geräts angibt, von dem das Ereignis generiert wurde.
Bay (Einschub)	Die Einschubsnummer des Geräts, von dem das Ereignis generiert wurde.
Perceived Severity (Wahrgenommener Schweregrad)	Eine Zeichenfolge, die den Schweregrad des Ereignisses angibt. Mögliche Werte sind: Critical Error (Kritischer Fehler), Degraded (Beeinträchtigt), Informational (Informativ).
Submission Status (Übermittlungsstatus)	Der Status der Ereignisübermittlung. Mögliche Werte sind OK oder ERROR (Fehler).

Löschen des Serviceereignis-Protokolls

Um den Inhalt des Serviceereignis-Protokolls zu löschen, klicken Sie auf **Clear Event Log** (Ereignisprotokoll löschen).

Insight Remote Support-Datensammlungen



Datensammlungsinformationen

HP Insight Online-Direktverbindung

Zeile	Beschreibung
Last Data Collection Transmission (Übertragung der letzten Datensammlung)	Datum und Uhrzeit der letzten erfolgreichen Datensammlung
Last Data Collection Status (Status der letzten Datensammlung)	Der Übertragungsstatus; mögliche Werte sind „OK“ oder „Error“ (Fehler)
Next Scheduled Data Collection (Nächste geplante Datensammlung)	Datum und Uhrzeit der nächsten geplanten Datensammlung; die Datensammlung wird automatisch in 30-tägigen Intervallen geplant

HP Insight Remote Support

Zeile	Beschreibung
Last Data Collection Transmission (Übertragung der letzten Datensammlung)	Datum und Uhrzeit der letzten erfolgreichen Datensammlung
Last Data Collection Status (Status der letzten Datensammlung)	Der Übertragungsstatus; mögliche Werte sind „OK“ oder „Error“ (Fehler)

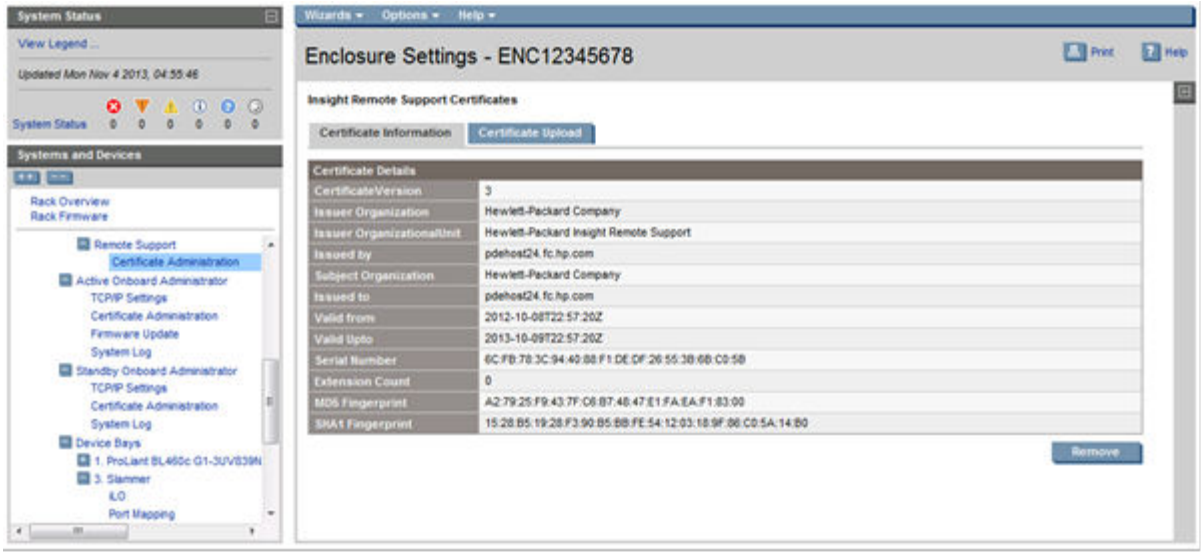
Wenn die Datensammlung unverzüglich an HP gesendet werden soll, klicken Sie auf **Send Data Collection** (Datensammlung senden). Zur Ausführung dieser Aufgabe werden Administratorrechte benötigt.

Zugehörige Themen

Insight Remote Support-Registrierung (Insight Remote Support-Registrierung auf Seite 184)

Insight Remote Support-Serviceereignisse (Insight Remote Support-Serviceereignisse auf Seite 192)

Remote Support-Zertifikatverwaltung



Registerkarte „Certificate Information“ (Zertifikatinformationen)

Dieser Bildschirm zeigt alle Insight Remote Support-Serverzertifikate an, die der Onboard Administrator als vertrauenswürdig ansieht. Auf den Onboard Administrator können maximal acht Zertifikate hochgeladen werden. Zertifikate stellen sicher, dass der Onboard Administrator Informationen sicher an den Insight Remote Control-Server sendet. Wenn keine Zertifikate verwendet werden, dann ist die Kommunikation für „Man-in-the-Middle“-Angriffe anfällig. Um sicherzustellen, dass das Zertifikat gültig ist und nicht modifiziert wurde, überprüfen Sie den SHA1-Fingerabdruck des Zertifikats mittels einer separaten Methode, einer E-Mail-Nachricht von dem Serveradministrator, einer Webseite oder einer anderen vertrauenswürdigen Quelle.

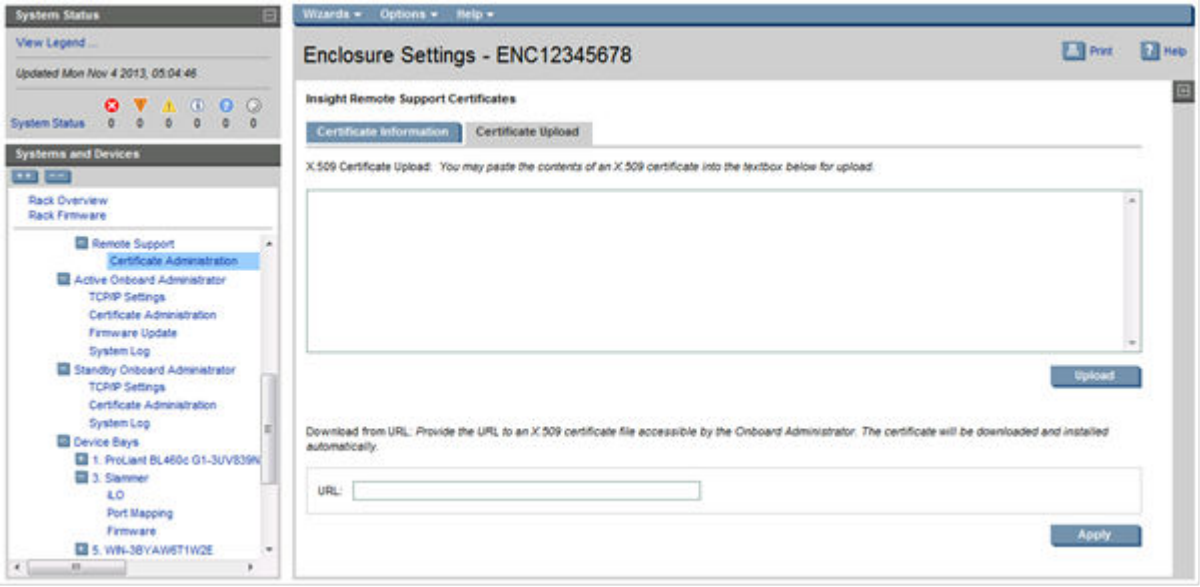
HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, ist beim Anschluss an ein HP Insight Remote Support-Hostgerät ein gültiges Zertifikat erforderlich.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

Zeile	Beschreibung
Certificate Version (Version des Zertifikats)	Die Versionsnummer des aktuellen Zertifikats.
Issuer Organization (Ausstellende Organisation)	Der Name der Organisation, die das Zertifikat ausgestellt hat.
Issuer Organization Unit (Ausstellende Organisationseinheit)	Der Name der Organisationseinheit, die das Zertifikat ausgestellt hat.
Issued by (Ausgestellt von)	Die Zertifizierungsstelle, die das Zertifikat ausgestellt hat.
Subject Organization (Fachorganisation)	Fachname
Issued To (Ausgestellt an)	Organisation, der das Zertifikat ausgestellt wurde.
Valid From (Gültig ab)	Das Datum, ab dem das Zertifikat gültig ist.
Valid Upto (Gültig bis)	Das Datum, an dem das Zertifikat abläuft.
Serial Number (Seriennummer)	Die dem Zertifikat von der Zertifizierungsstelle zugewiesene Seriennummer.
Extension Count (Verlängerungsanzahl)	Die Anzahl der Verlängerungen im Zertifikat.
MD5 Fingerprint (MD5-Fingerabdruck)	Anhand dieses Feldes kann die Authentizität des Zertifikats validiert werden
SHA1 Fingerprint (SHA1-Fingerabdruck)	Anhand dieses Feldes kann die Authentizität des Zertifikats validiert werden

Um ein bestehendes Zertifikat zu entfernen, klicken Sie auf **Remove** (Entfernen).

Remote Support-Registerkarte „Certificate Upload“ (Zertifikat-Upload)



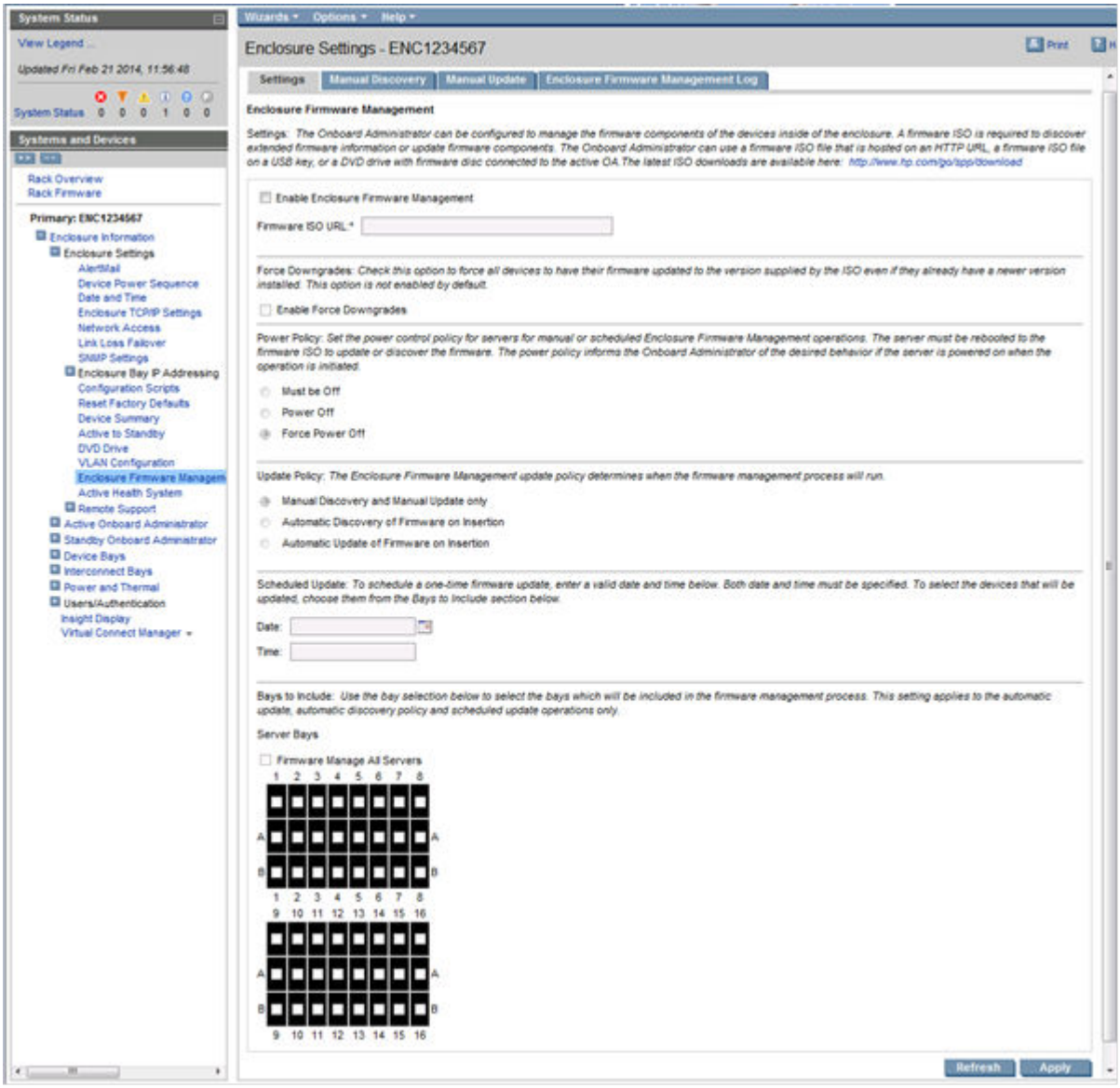
Registerkarte „Certificate Upload“ (Zertifikat-Upload)

Laden Sie das Zertifikat des Insight Remote Support-Servers auf den Onboard Administrator hoch.

Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Enclosure Firmware Management


System Status
View Legend ...
Updated Fri Feb 21 2014, 11:56:48
System Status 0 0 0 1 0 0
Systems and Devices
Rack Overview
Rack Firmware
Primary: ENC1234567
Enclosure Information
Enclosure Settings
AlertMail
Device Power Sequence
Date and Time
Enclosure TCP/IP Settings
Network Access
Link Loss Failover
SNMP Settings
Enclosure Bay IP Addressing
Configuration Scripts
Reset Factory Defaults
Device Summary
Active to Standby
DVD Drive
VLAN Configuration
Enclosure Firmware Managem
Active Health System
Remote Support
Active Onboard Administrator
Standby Onboard Administrator
Device Bays
Interconnect Bays
Power and Thermal
Users/Authentication
Insight Display
Virtual Connect Manager
Wizards
Options
Help
Enclosure Settings - ENC1234567
Print
Settings
Manual Discovery
Manual Update
Enclosure Firmware Management Log
Enclosure Firmware Management
Settings: The Onboard Administrator can be configured to manage the firmware components of the devices inside of the enclosure. A firmware ISO is required to discover extended firmware information or update firmware components. The Onboard Administrator can use a firmware ISO file that is hosted on an HTTP URL, a firmware ISO file on a USB key, or a DVD drive with firmware disc connected to the active OA. The latest ISO downloads are available here: http://www.hp.com/go/spp/download
Enable Enclosure Firmware Management
Firmware ISO URL:*
Force Downgrades: Check this option to force all devices to have their firmware updated to the version supplied by the ISO even if they already have a newer version installed. This option is not enabled by default.
Enable Force Downgrades
Power Policy: Set the power control policy for servers for manual or scheduled Enclosure Firmware Management operations. The server must be rebooted to the firmware ISO to update or discover the firmware. The power policy informs the Onboard Administrator of the desired behavior if the server is powered on when the operation is initiated.
Must be Off
Power Off
Force Power Off
Update Policy: The Enclosure Firmware Management update policy determines when the firmware management process will run.
Manual Discovery and Manual Update only
Automatic Discovery of Firmware on Insertion
Automatic Update of Firmware on Insertion
Scheduled Update: To schedule a one-time firmware update, enter a valid date and time below. Both date and time must be specified. To select the devices that will be updated, choose them from the Bays to Include section below.
Date:
Time:
Bays to Include: Use the bay selection below to select the bays which will be included in the firmware management process. This setting applies to the automatic update, automatic discovery policy and scheduled update operations only.
Server Bays
Firmware Manage All Servers
1 2 3 4 5 6 7 8
A
B
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
A
B
9 10 11 12 13 14 15 16
Refresh
Apply

Die Enclosure Firmware Management-Funktion (EFM) bietet einen einzelnen Ausgangspunkt zum Verwalten von Firmware auf unterstützten HP Servern und Verbindungsmodulen im Gehäuse. Folglich ermöglicht EFM Administratoren, für die Server Blades in einem Gehäuse eine einzelne Firmware-Baseline (SPP-Version) zu definieren. Die Firmware kann beim Einsetzen des Servers oder während eines vordefinierten Wartungsfensters auf die Baseline aktualisiert werden oder sie kann manuell aktualisiert werden. Onboard Administrator verwaltet Protokolle der EFM-Firmwareaktualisierungen und meldet, ob sie mit der eingerichteten Baseline konform sind.

Enclosure Firmware Management-Ausführung und -Berichterstellung

Während einer EFM-Firmwareaktualisierung der Geräte innerhalb des Gehäuses wird in verschiedene Phasen des Aktualisierungsvorgangs und bei der zugehörigen Verarbeitung, die auf dem OA-Modul ausgeführt werden, ein bedeutender Anteil der OA-Ressourcen (CPU, Arbeitsspeicher und Netzwerkdurchsatz) belegt. Dies gilt insbesondere bei dem Versuch, die Firmware mehrerer Blades im Gehäuse gleichzeitig zu aktualisieren. Die Ressourcen innerhalb des OA-Moduls reichen möglicherweise nicht aus, um die gleichzeitige Firmwareaktualisierung aller

Geräte innerhalb eines Gehäuses zu unterstützen. Daher ist es erforderlich, die momentanen Lastanforderungen zu kontrollieren, die die EFM-Verarbeitung an das OA-Module stellt. Zu diesem Zweck implementiert die OA-Firmware eine Art von Auftragssteuerung, die auf einer dynamischen Ressourcenverwaltungs-Heuristik basiert und mit der versucht wird, die Ressourcennutzung der EFM-bezogenen Verarbeitung auf ein Maß einzuschränken, bei dem die Fähigkeit des OA-Moduls zur Ausführung seiner anderen Gehäuse-Verwaltungsaufgaben nicht beeinträchtigt wird. Als Teil dieser Heuristik zur dynamischen Ressourcen-Verwaltung überwacht die OA-Firmware speziell die folgenden Faktoren:

- Prozessorauslastung (insbesondere der Prozessladedurchschnitt auf der im OA-Modul integrierten CPU)
- Speicherauslastung
- Anzahl der noch ausstehenden Übertragungen der Firmware-ISO auf die Blades über iLO Virtual Media.

Basierend auf diesen Faktoren aktualisiert die EFM-Auftragssteuerungslogik die Server nötigenfalls stapelweise. Dabei wird (1) die gleichzeitige Aktualisierung möglichst vieler Geräte innerhalb des Gehäuses in Übereinstimmung mit den eingerichteten Ressourcen-Grenzwerten ermöglicht, die durch die Heuristik zur dynamischen Ressourcenverwaltung geltend gemacht werden, und wird (2) die Aktualisierung von anderen Geräten verzögert, bis die Ressourcen wieder verfügbar sind. Bei dem Versuch, gleichzeitig mehrere Gehäusekomponenten zu aktualisieren, werden einige der Aktualisierungen möglicherweise nicht alle gleichzeitig durchgeführt. Der Zeitpunkt, zu dem mit der Batchverarbeitung begonnen wird, ist variabel und hängt von solchen Faktoren wie der Anzahl der für die Aktualisierung ausgewählten Geräte, bestimmten Aspekte des Verwaltungsnetzwerks wie z. B. Menge und Typ des Datenverkehrs, der spezifischen OA-Konfiguration, anderen ausstehenden Verwaltungsaktivitäten, die von OA durchgeführt werden, sowie von allen anderen Faktoren ab, die sich auf die Ressourcennutzung auf dem OA-Modul auswirken, wenn die EFM-Aktualisierung gestartet wird. Hinweise auf eine solche Batchverarbeitung könnten bestimmte im Firmwareprotokoll gemeldete Verzögerungen sein.

Weitere Informationen zum Firmwareprotokoll und anderen Firmwareverwaltungsprotokollen finden Sie unter „Firmwareverwaltungsprotokolle“ (Firmware-Management-Protokolle auf Seite 275).

EFM und Integration mit HP SUM

EFM erkennt und aktualisiert die Firmware durch Starten eines Servers über ein unterstütztes HP SPP-ISO-Image. EFM nutzt das im SPP-ISO integrierte HP SUM-Modul und erzielt dabei ähnliche Ergebnisse wie bei einer manuellen Ausführung von HP SUM, mit dem Unterschied, dass durch Zentralisieren der Steuerung und durch Erkennen und Aktualisieren der Firmware auf mehreren Servern jedoch Zeit eingespart wird.

Sollte während der Ausführung einer EFM-Aufgabe ein zugehöriger HP SUM- oder EFM-Vorgang fehlschlagen, leitet EFM automatisch eine Wiederholung der gesamten EFM-Aufgabe ein. EFM versucht insgesamt drei Mal, die Aufgabe auszuführen. Bei den Wiederholungsversuchen werden zuvor in der EFM-Aufgabe durchgeführte Schritte möglicherweise wiederholt, je nachdem, an welcher Stelle der Fehler aufgetreten ist. Wenn die Aufgabe bei dem letzten Versuch nicht erfolgreich durchgeführt werden kann, wird die EFM-Aufgabe mit einem fehlgeschlagenen Status abgebrochen.

HINWEIS: In seltenen Fällen kann es vorkommen, dass EFM-Protokolle eine erfolgreiche Durchführung der gesamten EFM-Aufgabe angeben, obwohl die HP SUM-Prozesse aufgrund eines Fehlers abgebrochen wurden. Die Firmwareversionen werden nicht wie erwartet aktualisiert. Dies kann anhand einer Diskrepanz zwischen den gemeldeten installierten Firmwareversionen und den im verwendeten Firmware-ISO verfügbaren Firmwareversionen festgestellt werden. Wenn eine solche Diskrepanz auftritt, empfiehlt HP, die Firmware- und Sitzungsprotokolle auf Anzeichen eines HP SUM-Fehlers zu überprüfen. Wenn ein Fehler angegeben wird, könnte die EFM-Aufgabe ebenfalls fehlgeschlagen sein. Weitere Informationen zu EFM-Protokollen finden Sie unter „Firmwareverwaltungsprotokolle“ (Firmware-Management-Protokolle auf Seite 275). Weitere Informationen zu EFM-Fehlern finden Sie unter „Enclosure Firmware Management-Protokoll“ (Enclosure Firmware Management-Protokoll auf Seite 205). Weitere Informationen zum Anzeigen von Firmwareversionen finden Sie unter „Anzeigen der Firmwareversionen“ (Anzeigen der Firmware-Versionen auf Seite 277).

Andere Vorsichtsmaßnahmen bezüglich der Verarbeitungsleistung

Enclosure Firmware Management funktioniert nicht zuverlässig und sollte auf langsamen Netzwerkverbindungen (weniger als 1 GB) nicht verwendet werden.

Während der Ausführung von Enclosure Firmware Management-Vorgängen ist die Onboard Administrator-Reaktionszeit möglicherweise langsamer als gewöhnlich und der Gerätestatus kann kurzzeitig als beeinträchtigt gemeldet werden. Meldungen oder Warnmeldungsbedingungen dieser Art können bedenkenlos ignoriert werden, während die Vorgänge ausgeführt werden.

HINWEIS: Die Leistung von HP c-Class BladeSystem ProLiant und Integrity iLO Virtual Media wird basierend auf der Aktivität und Anzahl gleichzeitiger iLO Virtual Media-Sitzungen und der Onboard Administrator-Auslastung eingeschränkt. Die Onboard Administrator-Funktionen „Enclosure DVD Management“ (Gehäuse-DVD-Verwaltung) und „Enclosure Firmware Management“ (Gehäuse-Firmware-Verwaltung) nutzen ebenfalls die iLO-Funktion virtueller Medien und weisen ähnliche Leistungseinschränkungen auf. Um Zeitüberschreitungsprobleme der Medien zu vermeiden, empfiehlt HP, die Anzahl gleichzeitiger Sitzungen einzuschränken. Sollten während der Betriebssysteminstallation oder während Firmwareaktualisierungen Zeitüberschreitungsprobleme auftreten, dann verringern Sie die Anzahl laufender virtueller Medien-Sitzungen und starten Sie den Vorgang neu.

HINWEIS: In seltenen Fällen können während einer EFM-Aufgabe bestimmte serverseitige Fehler (z. B. ein abgestürzter iLO Firmware-Aktualisierungsvorgang oder eine übermäßig lange Ausführungszeit) auftreten, ohne dass für den betreffenden EFM-Prozess Fehler angegeben werden. Sollten solche Fehler auftreten, wird die OA-EFM-Aufgabe nicht abgeschlossen und scheint ohne gemeldeten Fortschritt oder Status abgestürzt zu sein. Starten Sie zum Beheben dieses Zustands das aktive OA-Modul neu, oder führen Sie ein manuelles Failover auf das redundante OA-Modul durch.

Enclosure Firmware Management-Einstellungen

Enclosure Firmware Management-Einstellungen sind Benutzern mit Onboard Administrator-Administratorberechtigungen vorbehalten und sind auf der Onboard Administrator-GUI auf der Seite **Enclosure Settings (Gehäuseeinstellungen)>Enclosure Firmware Management** oder über die Onboard Administrator CLI verfügbar.

Erforderliche Benutzerberechtigungen

Alle Enclosure Firmware Management-Funktionen sind über die Onboard Administrator-GUI- und CLI verfügbar, sofern für das Blade im Gehäuse nicht „Secure Boot“ (Sicherer Systemstart) aktiviert ist. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer daran, Startoptionen abzuändern oder Startvorgänge über die Onboard Administrator-GUI oder -CLI auszuführen. Diese Aufgaben müssen über das vom Administrator in BIOS konfigurierte Gerät durchgeführt werden.

Benutzerrolle und Einschubsberechtigungen des Onboard Administrators steuern die Enclosure Firmware Management-Einstellungen und die Fähigkeit, Firmware-Informationen anzuzeigen.

Benutzerrolle	Einstellungen oder geplante Aktualisierung ändern	Manuelle Ermittlung oder Aktualisierung starten	Firmware-Versionen anzeigen
Onboard Administrator-Administrator oder -Bediener	Ja	Ja, nur OA-Administrator*	Ja
Server-Administrator oder -Bediener	Nein	Ja, nur OA-Administrator*	Ja, für berechtigte Server-Einschübe
Onboard Administrator-Benutzer	Nein	Nein	Ja, für berechtigte Einschübe

* Wenn für das Blade im Gehäuse der Modus „Secure Boot“ (Sicherer Systemstart) aktiviert ist, kann dieser Vorgang nicht über die GUI oder CLI durchgeführt werden.

Aktivieren des Enclosure Firmware Management

Das Kontrollkästchen **Enable Enclosure Firmware Management** (Enclosure Firmware Management aktivieren) aktiviert oder deaktiviert (Standardeinstellung) global das Enclosure Firmware Management. Wenn es deaktiviert ist, können keine manuellen Enclosure Firmware Management-Vorgänge gestartet werden. Alle zuvor konfigurierten automatischen oder geplanten Vorgänge finden nicht statt. Wenn die Einstellung von aktiviert in deaktiviert geändert wird, werden alle laufenden Enclosure Firmware Management-Ermittlungen oder -Aktualisierungen fortgesetzt, bis sie abgeschlossen sind.

HINWEIS: Einmal auf einem Server gestartete Enclosure Firmware Management-Vorgänge können nicht mehr gestoppt werden. Stellen Sie sicher, dass Ihr Gehäuse IPv6-kompatibel ist, bevor Sie eine IPv6-Adresse für das Firmware-Management-ISO-Image verwenden.

Das Enclosure Firmware Management wird auf den folgenden Onboard Administrator-Hardwaremodulen nicht unterstützt:

- HP BladeSystem c3000 Onboard Administrator (HP Teilenummer 448589-B21, 461514-B21)
- HP BladeSystem c7000 Onboard Administrator (HP Teilenummer 412142-B21)

Enclosure Firmware Management kann nur aktiviert werden, wenn das aktive Onboard Administrator-Hardwaremodul unterstützt wird. Bei dem Versuch, Enclosure Firmware Management bei nicht unterstütztem aktiven Onboard Administrator zu aktivieren, erscheint folgende Fehlermeldung:

```
Enclosure Firmware Management is not supported on the active OA hardware
present.
```

Wenn das Standby-Onboard Administrator-Modul nicht unterstützt wird, erscheint folgende Warnmeldung:

```
Enclosure Firmware Management is not supported on the standby OA hardware
present. The feature will be disabled if the standby OA becomes Active.
(Diese Funktion wird deaktiviert, wenn das OA-Standby-Modul aktiv wird.)
```

Enclosure Firmware Management schlägt auf jedem Blade fehl, wenn SSH in den Blade-iLO-Konfigurationseinstellungen deaktiviert ist. Standardmäßig ist SSH in iLO aktiviert.

Konfigurieren des Speicherortes des Firmware-Images

Zum Durchführen von Firmware-Erkennung oder Firmware-Aktualisierungen benötigt Enclosure Firmware Management ein Firmware-ISO-Abbild. Sie können eine die folgenden Positionen für das ISO-Firmware-Abbild angeben:

- Ein HTTP URL-basiertes ISO-Image, das auf einem Webserver gehostet wird Geben Sie eine IPv4-Adresse im folgenden Format an: `Protokoll://[< IPv4-Adresse >]/Pfad/Dateiname`. Um eine IPv6 URL-Adresse anzugeben, geben Sie die Adresse in Klammern im folgenden Format an: `Protokoll://[<IP-Adresse>]/Pfad/Dateiname`.

  Die maximale Länge der URL beträgt 511 Zeichen.

- Ein USB-Schlüssel mit dem ISO Image, der an dem USB-Port des Onboard Administrators angeschlossen wird.

  Ein USB-Schlüssel, der von dem SPP-ISO-Image in startfähige Medien umgewandelt wurde, wird beim Enclosure Firmware Management nicht unterstützt. Der USB-Schlüssel muss das ISO-Image im Stammverzeichnis enthalten. Die maximale unterstützte USB-Schlüsselgröße ist 4 GB. Wenn eine physische DVD verwendet wird, darf die DVD kein ISO-Image enthalten. Die DVD muss ein vom ISO-Image erstellter startfähiger Datenträger sein. Die aktuellen ISO-Downloads sind auf der HP-Website verfügbar (http://www.hp.com/go/spp/download).

- Eine physische DVD, die in das DVD-Laufwerk des Gehäuses eingelegt wird.

Onboard Administrator unterstützt nur SPP-ISO-Images kleiner als 4 GB. Bei SPP-ISO-Images gleich oder größer als 4 GB müssen Sie ein benutzerdefiniertes ISO-Image erstellen, aus dem die Komponenten ausgeschlossen werden, die für die OA-EFM-Blade-Firmwareaktualisierung nicht benötigt werden. Weitere Informationen finden Sie im folgenden Abschnitt.

Erstellen eines benutzerdefinierten SPP-ISO-Image

Die folgenden Anleitungen bieten die grundlegende Schritte zum Erstellen eines benutzerdefinierten SPP-ISO-Image für die Onboard Administrator-EFM-Funktionalität. Es wird davon ausgegangen, dass Sie über Erfahrung mit HP SUM zum Erstellen von benutzerdefinierten ISO-Images verfügen. Weitere Informationen finden Sie in der HP SUM-Onlinehilfe oder im Whitepaper *Building and deploying a customized SPP firmware ISO image* (Erstellen und Bereitstellen eines benutzerdefinierten SPP-Firmware-ISO-Image) und in anderer Dokumentation auf der HP Enterprise Library-Website (http://www.hp.com/go/hpsum/documentation).

1. Laden Sie das SPP-ISO-Image mit HP SUM 7.2 (oder höher) in einen Ordner auf Ihrem lokalen Laufwerk herunter.
2. Starten Sie die HP SUM-Stapeldatei.
3. Wählen Sie im Menü **Options** (Optionen) **Baseline Library** (Baseline-Bibliothek). Das SPP wird automatisch als Baseline hinzugefügt. Warten Sie mit dem nächsten Schritt, bis HP SUM angezeigt wird und die Bestandsaufnahme für die Baseline beendet hat.
4. Wählen Sie auf der Registerkarte **Actions** (Aktionen) der Baseline-Bibliothek **Create Custom** (Benutzerdefinierte erstellen).
5. Geben Sie die erforderlichen Angaben im Bereich **Overview** (Übersicht) des Fensters „Create Custom Baseline“ (Benutzerdefinierte Baseline erstellen) ein.
   - Geben Sie unter **Output Location** (Ausgabespeicherort) den Speicherort an, an dem das benutzerdefinierte ISO-Image platziert werden soll. Sie können auch zu dem gewünschten Speicherort navigieren.
   - Klicken Sie für **Extracted Source ISO Location** (Speicherort des extrahierten Quell-ISO) auf **Browse** (Durchsuchen), um das Quell-SPP-ISO-Image auszuwählen, dass angepasst werden soll.
   - Aktivieren Sie das Kontrollkästchen **Make Bootable ISO file** (Startfähige ISO-Datei erstellen).
6. Im Bereich **Step 2 - Filters** (Schritt 2 – Filter):

a. Wählen Sie für **Component Type** (Komponententyp) **Firmware** aus.

b. Aktivieren Sie alle Kontrollkästchen (**Critical Updates** (Kritische Updates), **Recommended Updates** (Empfohlene Updates), **Optional Updates** (Optionale Updates)).

7. Klicken Sie auf **Advanced Filter** (Erweiterter Filter), und wählen Sie die erforderlichen Filter aus.

   Wählen Sie für **Server Model** (Servermodell) **HP ProLiant BL Series**.

8. Klicken Sie im Bereich **Step 3 - Review** (Schritt 3 – Überprüfung) auf **Apply Filters** (Filter anwenden).

   Warten Sie, bis alle gefilterten Komponenten abgerufen wurden. Der Status des Abrufvorgangs kann unten auf der Seite angezeigt werden. Wenn der Vorgang abgeschlossen wurde, wird die Meldung „`Completed retrieving components`“ angezeigt.

9. Klicken Sie auf „Create ISO“ (ISO erstellen).

Nach wenigen Minuten ist das angepasste SPP-ISO-Abbild an dem zuvor unter **Output Location** (Ausgabespeicherort) angegebenen Speicherort einsatzbereit.

Aktivieren erzwungener Downgrades

Das Kontrollkästchen „Enable Force Downgrades“ (Erzwungene Downgrades aktivieren) aktiviert oder deaktiviert (Standardeinstellung) erzwungene Herabstufungen. Wenn es deaktiviert ist, werden Komponenten mit höheren Firmware-Versionen als die auf dem ISO-Image vorhandenen Firmware-Versionen aus der Aktualisierung ausgeschlossen. Diese Einstellung gilt für alle unterstützten Server Blades in diesem Gehäuse. Wenn es aktiviert ist, weist Enclosure Firmware Management das HP SUM-Modul an, die Flash-Aktualisierung von Komponenten-Firmware höherer Versionen als die Versionen im Image zu ermöglichen. Durch Aktivieren dieser Einstellung wird nicht garantiert, dass die Komponenten-Firmware herabgestuft wird. Wenn Sie die Option „Enable Force Downgrades“ (Erzwungene Downgrades aktivieren) verwenden, schlagen Sie vorher in der ISO-Dokumentation nach, welche Erwartungen realistisch sind.

Einstellen der Stromversorgungsrichtlinie

Der Server muss über das ISO-Image gestartet werden, damit die Firmware aktualisiert oder ermittelt wird. Die Stromversorgungsrichtlinie teilt dem Onboard Administrator mit, welche Maßnahme zu ergreifen ist, wenn der Server beim Starten des Vorgangs eingeschaltet ist. Diese Einstellung trifft auf geplante und manuelle Vorgänge zu. Die Standard-Stromversorgungsrichtlinie ist **Must be Off** (Muss ausgeschaltet sein).

Wenn für die Stromversorgungsrichtlinie „Power Off“ (Ausschalten) eingestellt ist, wartet der Onboard Administrator fünf Minuten lang auf eine Antwort des Servers auf die Anforderung. Wenn der Server innerhalb dieses Zeitraums nicht heruntergefahren wird, schlägt der Firmware-Management-Vorgang fehl. Wenn der Server ein Betriebssystem ausführt, durch das das Herunterfahren gestartet, aber nicht innerhalb von fünf Minuten zu Ende geführt wurde, wird der Server möglicherweise heruntergefahren und bleibt ausgeschaltet.

Einstellung	Beschreibung
Must be Off (Muss ausgeschaltet sein)	Der Onboard Administrator bricht den Vorgang ab, wenn der Server eingeschaltet ist.

Einstellung	Beschreibung
Power Off (Ausschalten)	Der Onboard Administrator ahmt ein kurzes physisches Drücken des Netzschalters am Server Blade nach, wodurch der Server Blade ordnungsgemäß heruntergefahren wird.
Force Power Off (Ausschalten erzwingen)	Der Onboard Administrator ahmt ein physisches Drücken und Halten des Netzschalters am Server Blade nach, wodurch der Server Blade zum Ausschalten gezwungen wird, ohne zuerst das Betriebssystem herunterzufahren.

⚠ ACHTUNG: Die Richtlinie „Force Power Off“ (Ausschalten erzwingen) ist auf Servern mit einem installierten Betriebssystem mit Vorsicht zu verwenden, da dies zu einer Datenbeschädigung führen kann.

Einstellen der Aktualisierungsrichtlinie

Für das Firmware-Management sind die folgenden Aktualisierungsrichtlinien verfügbar:

- Manual Discovery and Manual Update Only (Nur manuelle Ermittlung und manuelle Aktualisierung): Die Standardrichtlinie. Diese Richtlinie verhindert, dass der Onboard Administrator die Server-Aktualisierung und -Ermittlung beim Einsetzen in das Gehäuse automatisch durchführt.

  Es ist eine manuelle Ermittlung oder Aktualisierung und eine geplante Aktualisierung erforderlich, damit der Onboard Administrator erweiterte Server-Firmwareversionen anzeigen kann.

- Automatic Discovery on Insertion (Automatische Ermittlung beim Einsetzen): Ermöglicht dem Onboard Administrator, einen Systemstart für die Ermittlung auf einem aktivierten Server durchzuführen, wobei die einzuschließenden Einschübe verwendet, erweiterte Firmware-Informationen für den betreffenden Server erfasst, das Firmware-Management-Protokoll für das betreffende Ereignis aktualisiert und dann der Server in den normalen Betriebszustand neu gestartet wird. Sie können dann die ermittelten Firmwareversionen anzeigen und die betreffende Firmware über eine manuelle oder eine geplante Aktualisierung aktualisieren.

- Automatic Update on Insertion (Automatische Aktualisierung beim Einsetzen): Ermöglicht dem Onboard Administrator, einen Systemstart für die Aktualisierung auf einem aktivierten Server durchzuführen, wobei die einzuschließenden Einschübe verwendet, erweiterte Firmware-Informationen für den betreffenden Server erfasst, das Firmware-Management-Protokoll für das betreffende Ereignis aktualisiert und dann der Server in den normalen Betriebszustand neu gestartet wird. Diese Richtlinie aktualisiert die Server-Firmware nach einem Service-Ereignis, wie z. B. Auswechseln der Serverkarte oder der Optionskarte, auf das ausgewählte Firmware-Image.

Die automatische Ermittlung und automatische Aktualisierung sind sich gegenseitig ausschließende Richtlinien und betreffen alle im Gehäuse einzuschließenden Einschüben.

Festlegen einer geplanten Firmwareaktualisierung

Die Richtlinie einer geplanten Firmwareaktualisierung bietet dem Onboard Administrator einen Plan, mit dem alle einzuschließenden Einschübe automatisch auf die Firmwareversionen auf dem ISO-Firmware-Image aktualisiert werden. Am geplanten Datum und zur geplanten Uhrzeit startet der Onboard Administrator einen Aktualisierungsvorgang, wobei die Stromversorgungsrichtlinie auf allen einzuschließenden Einschüben verwendet und deren Firmware anhand des ISO-Firmware-Image aktualisiert wird und dann alle eingeschlossenen Server wieder in den normalen Betriebszustand neu gestartet werden.

Angeben der in einem Firmware-Verwaltungsvorgang aufzunehmenden Einschübe

Alle Geräteeinschübe werden standardmäßig im Firmware-Management eingeschlossen. Der Administrator von Onboard Administrator kann bestimmte einzuschließende Geräteeinschübe auswählen oder die Auswahl anderer Geräteeinschübe aufheben, die in Enclosure Firmware Management-Aktualisierungsrichtlinien, manuellen Aktualisierungen oder geplanten Aktualisierungen ausgeschlossen werden müssen.

Das Kontrollkästchen **Firmware Manage All Servers** (Firmware verwaltet alle Server) ist standardmäßig aktiviert. Dadurch wird die Ausführung von Enclosure Firmware Management-Richtlinien und geplanten Aktualisierungen auf allen verfügbaren Servern ermöglicht.

Sie können jeden der Basis-Einschübe, Einschübe der Seite a und Einschübe der Seite b einzeln auswählen oder das Kontrollkästchen **Firmware Manage All Servers** (Firmware verwaltet alle Server) aktivieren, wenn alle Geräteeinschübe ausgewählt werden sollen.

So wählen Sie bestimmte Server manuell für das Enclosure Firmware Management aus:

1. Deaktivieren Sie das Kontrollkästchen **Firmware Manage All Servers** (Firmware verwaltet alle Server).
2. Aktivieren Sie das Kontrollkästchen neben den einzelnen Einschüben oder wählen Sie Einschübe gemäß Einschubstyp aus.
3. Klicken Sie auf **Apply** (Übernehmen). Die aktualisierte Liste der im Enclosure Firmware Management einzuschließenden Einschübe erscheint.

Die Einschubsauswahl ist derzeit nur auf Geräteeinschübe eingeschränkt. Switch- und Onboard Administrator-Einschübe können nicht ausgewählt werden.

Die Option „Bays to Include“ (Einzuschließende Einschübe) trifft nur auf ProLiant Server Blades zu. Integrity Server Blades unterstützen diese Funktion nicht. Die Unterstützung für Partner-Blades wird über den zugehörigen Server Blade basierend darauf bereitgestellt, ob das Firmware-ISO-Image die PCIe-Adapterkarte im Partner-Blade unterstützt.

Enclosure Firmware Management-Protokoll

Informationen zu Firmwareprotokollen, einschließlich des Enclosure Firmware Management-Protokolls, finden Sie unter „Firmware-Management-Protokolle“ (Firmware-Management-Protokolle auf Seite 275).

Manuelle Ermittlung

Die manuelle Ermittlung eines oder mehrerer Server kann gestartet werden, um die Erfassung bestehender Firmwareversionen zu vereinfachen.

Nachdem eine manuelle Firmware-Ermittlung gestartet wurde, erscheint der Bildschirm „Manual Discovery Device Bay Selection“ (Geräteeinschubsauswahl für manuelle Ermittlung). Wählen Sie einen oder mehrere Geräteeinschübe aus, auf denen die Ermittlung durchgeführt werden soll. Sie können auch das Kontrollkästchen **Discover All Servers** (Alle Server ermitteln) aktivieren, um alle Server für die Ermittlung auszuwählen. Standardmäßig sind alle Geräteeinschübe und das Kontrollkästchen „Discover All Servers“ (Alle Server ermitteln) ausgewählt.

Wenn „Secure Boot“ (Sicherer Systemstart) auf einem Server Blade konfiguriert ist, kann der zugehörige Einschub nicht ausgewählt werden (es wird das Symbol eines Vorhängeschlosses angezeigt). Der Modus „Secure Boot“ (Sicherer Systemstart) hindert Benutzer daran, eine manuelle Ermittlung über die Onboard Administrator-GUI oder-CLI durchzuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Um den Ermittlungsvorgang auf den ausgewählten Servern zu starten, klicken Sie auf **Start Manual Discovery** (Manuelle Ermittlung starten).

Manuelle Aktualisierung

Es kann ein manuelles Update eines oder mehrerer Server zu den angegebenen Firmware-Image-Version initiiert werden. Um eine Firmwareaktualisierung auf einem oder mehreren Servern zu starten, klicken Sie auf **Manual Update** (Manuelle Aktualisierung).

Nachdem eine manuelle Firmwareaktualisierung gestartet wurde, erscheint der Bildschirm „Manual Update Device Bay Selection“ (Geräteeinschubsauswahl für manuelle Aktualisierung). Wählen Sie einen oder mehrere Geräteeinschübe aus, auf denen die Aktualisierung durchgeführt werden soll. Sie können auch das Kontrollkästchen **Update All Servers** (Alle Server aktualisieren) aktivieren, um alle Server für die Aktualisierung auszuwählen. Standardmäßig sind alle Geräteeinschübe und das Kontrollkästchen „Discover All Servers“ (Alle Server ermitteln) ausgewählt.

Wenn „Secure Boot“ (Sicherer Systemstart) auf einem Server Blade konfiguriert ist, kann der zugehörige Einschub nicht ausgewählt werden (es wird das Symbol eines Vorhängeschlosses angezeigt). Der Modus „Secure Boot“ (Sicherer Systemstart) hindert Benutzer daran, eine manuelle Aktualisierung über die Onboard Administrator-GUI oder -CLI durchzuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Um den Aktualisierungsvorgang auf den ausgewählten Servern zu starten, klicken Sie auf **Start Manual Update** (Manuelle Aktualisierung starten).

Enclosure Firmware Management-Protokoll

Das Enclosure Firmware Management-Protokoll bietet eine konsolidierte Ansicht der wichtigsten Enclosure Firmware Management-Ereignisse, wie z. B. Firmware-Image-Auswahl, Richtlinien- und Zeitplanänderungen sowie gestartete und abgeschlossene Firmware-Vorgänge. Dieses Protokoll enthält nicht die schrittweisen Details, die im Firmware-Protokoll eines jeden Servers enthalten sind.

Das Enclosure Firmware Management-Protokoll ist über OA-Neustarts und Stromausfälle hinweg beständig. Es wird auf dem Standby-OA beibehalten, falls vorhanden.

Um aktualisierte Protokollinformationen anzuzeigen, klicken Sie auf **Refresh** (Aktualisieren).

Um Informationen für das Enclosure Firmware Management-Protokoll und das serverspezifische Firmware- und Sitzungsprotokoll zu löschen, klicken Sie auf **Clear All Logs** (Alle Protokolle löschen). (Weitere Informationen zum Firmware- und Sitzungsprotokoll finden Sie unter „Firmware Management-Protokolle“ (Firmware-Management-Protokolle auf Seite 275).

Um Informationen für das Enclosure Firmware Management-Protokoll zu löschen, klicken Sie auf **Clear Log** (Protokoll löschen).

⚠ **ACHTUNG:** Einmal gelöschte Daten können nicht wiederhergestellt werden.

Fehlgeschlagene Ereignisse

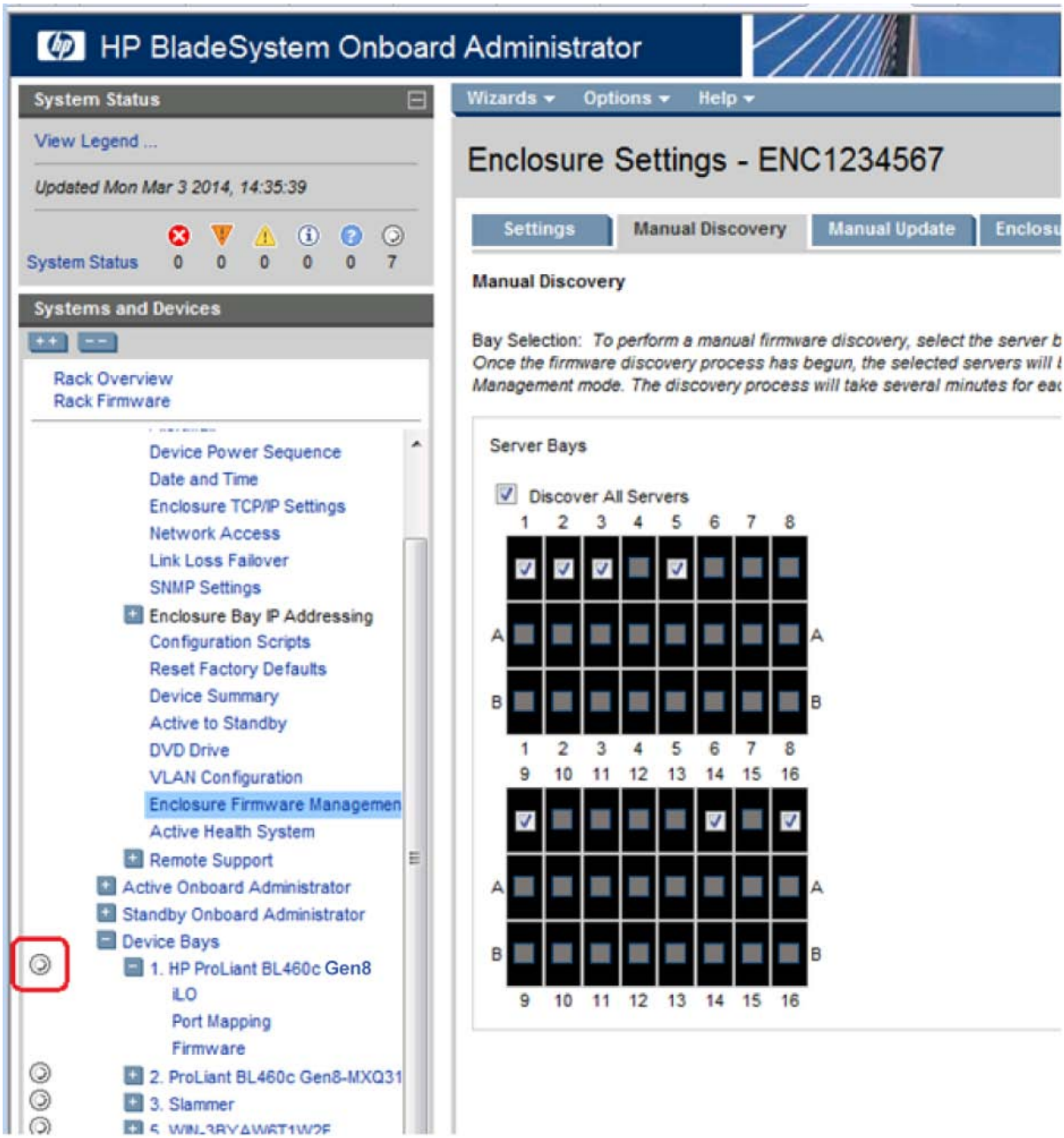
Wenn die Aufgabe „Enclosure Firmware Management“ auf einem Server abgeschlossen wurde, wird als letztes Ereignis im Server-Firmware-Protokoll `Firmware Management successfully completed` (Firmware-Management erfolgreich abgeschlossen) oder `Firmware Management is incomplete` (Firmware-Management unvollständig) aufgelistet.

Wenn für den zuletzt im Enclosure Firmware Management-Protokoll aufgeführten Vorgang keine erfolgreiche Ausführung angegeben wird, geben die anderen Firmware-Protokolleinträge möglicherweise über das von dem Onboard Administrator vorgefundene Problem Auskunft. So muss der Server beispielsweise ausgeschaltet werden, bevor eine manuelle Ermittlung, eine manuelle Aktualisierung oder eine geplante Aktualisierung durchgeführt wird. Aus dem Protokoll geht möglicherweise hervor, dass der Server eingeschaltet war und der Enclosure Firmware Management-Vorgang daher gestoppt wurde.

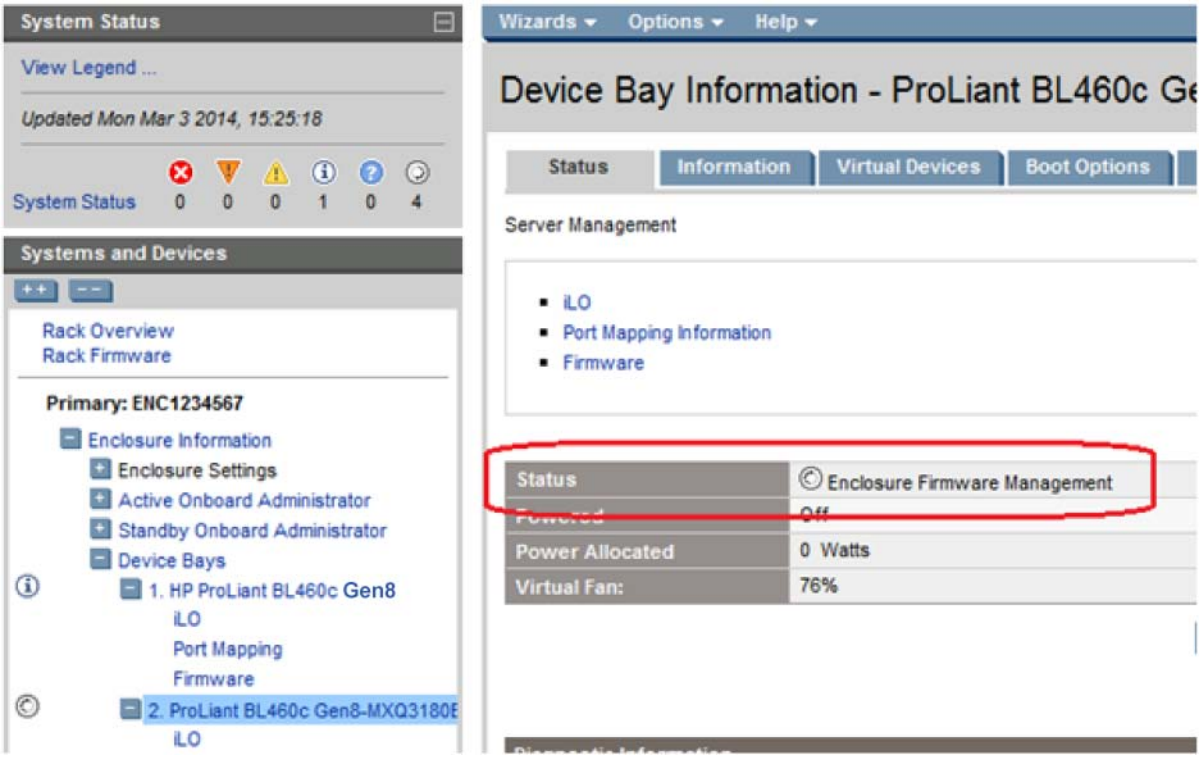
Wenn während der Durchführung der Aufgabe „Enclosure Firmware Management“ ein Fehler auftritt, wird der Fehler als `Firmware Management failed on blade X` (Firmware-Management auf Blade X fehlgeschlagen) protokolliert. Der Onboard Administrator wiederholt den Vorgang maximal dreimal. Wenn die Aufgabe abgeschlossen wird, können die vorherigen Protokoll-Fehlereinträge ignoriert werden. Detaillierte Informationen zum Ereignis und zur aktuellen Aktivität finden Sie im Firmware-Protokoll des Servers.

Statusaktualisierungen

Wenn eine Enclosure Firmware Management-Aufgabe, wie z. B. die manuelle Ermittlung oder die manuelle Aktualisierung auf einem Server gestartet wird, erscheint im linken Navigationsbereich neben jedem betroffenen Gerät ein Enclosure Firmware Management-Statussymbol. In der folgenden Abbildung wird eines von mehreren dieser Symbole rot eingekreist.



Während die Enclosure Firmware Management-Aufgabe verarbeitet wird, zeigt die Registerkarte „Device Bay Status“ (Geräteeinschubsstatus) (Registerkarte „Device Bay Status“ (Status des Geräteeinschubs) auf Seite 240) als Serverstatus wie in der folgenden Abbildung dargestellt `Firmware Management` an.



Wenn die Aufgabe abgeschlossen ist, wird als Serverstatus die entsprechende Angabe zurückgegeben. Um die Bedeutung der Statussymbole anzuzeigen, klicken Sie oben im linken Navigationsbereich auf **View Legende...** (Legende anzeigen).

Die erweiterten Server-Firmware-Informationen weisen einen Uhrzeit-/Datumsstempel für den Zeitpunkt auf, an dem der Ermittlungs- oder Aktualisierungsvorgang abgeschlossen wurde. Die Informationen werden zusammen mit einem Protokoll des letzten Firmware-Management-Ereignisses an einem beständigen Speicherort im Onboard Administrator abgelegt. Firmware-Informationen und -Protokoll werden zudem mit dem Standby-Onboard Administrator synchronisiert, sofern vorhanden.

Verwalten von Gehäusen

Ausschalten des Gehäuses

Es gibt zwei Methoden zum Ausschalten eines Gehäuses:

- Schalten Sie das PDU aus, über das das Gehäuse mit Strom versorgt wird.
- Ziehen Sie den (die) Netzstecker des Gehäuses heraus.

Onboard Administrator verfügt über keine virtuelle Methode zum Herunterfahren des Gehäuses.

Verbinden von Gehäusen

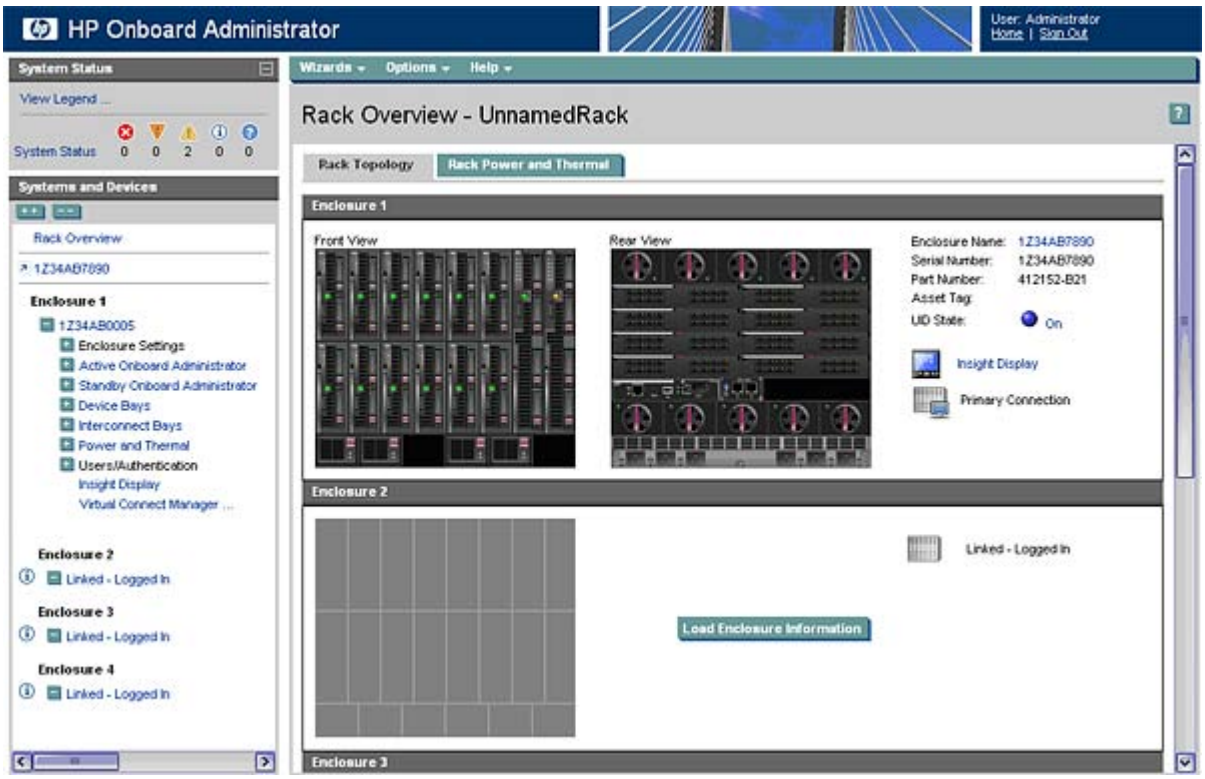
Gehäuse können über die Rückseite verbunden werden. Weitere Informationen finden Sie im betreffenden HP BladeSystem c7000 Gehäuse Setup- und Installationshandbuch.

Verwalten von mehreren Gehäusen

Im Hauptmenü innerhalb des Abschnitts „Systems and Devices“ (Systeme und Komponenten) des Bildschirms wird jedes Gehäuse durch seinen eindeutigen Namen identifiziert (der Standardgehäusename ist die Seriennummer des Gehäuses). Wenn Sie auf das blaue Kästchen mit einem Pluszeichen (+) klicken, wird die Gehäuseansicht erweitert, und Sie erhalten Zugriff auf die Unterkategorien für die verschiedenen Blades, Lüfter, Netzteile, Onboard Administrator-Module und Switches innerhalb des Gehäuses.

Um physikalisch zu ermitteln, mit welchem Gehäuse Sie arbeiten, klicken Sie auf die Schaltfläche „UID“ von Onboard Administrator. Wenn die Schaltfläche „UID“ gedrückt wird, leuchtet am Fach eine helle blaue LED auf. Um die UID auszuschalten, drücken Sie ein zweites Mal die Taste „UID“ am Onboard Administrator-Modul. Sie können an zwei Stellen im Gehäuse-Bildschirm feststellen, mit welchem Gehäuse Sie derzeit verbunden sind (im Bild hervorgehoben).

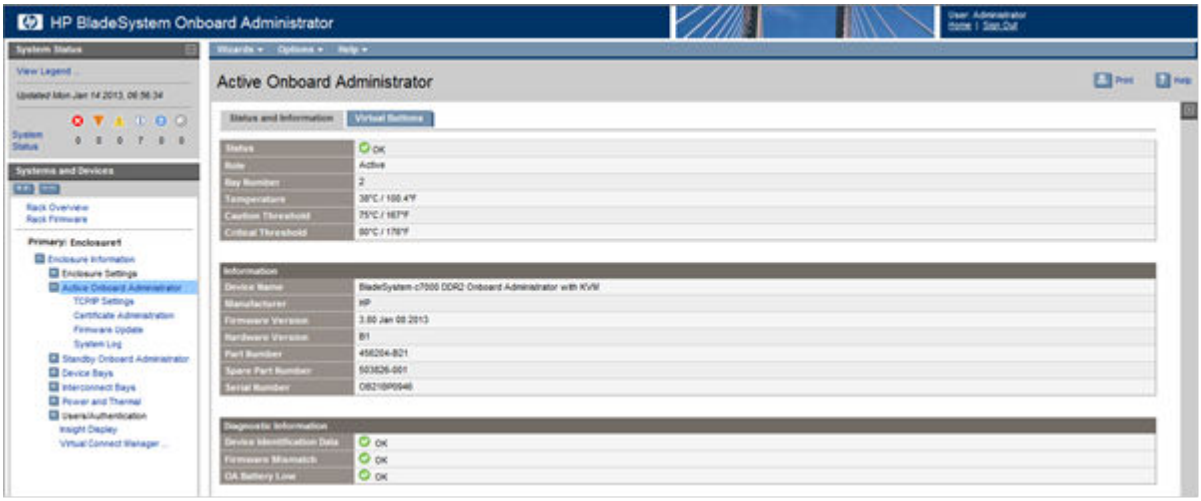
- Unter „Rack Overview“ (Rack-Übersicht) wird der Name des Gehäuses, bei dem Sie angemeldet sind, angezeigt.
- In der Liste der Gehäuse wird für das Gehäuse, bei dem Sie angemeldet sind, die Information „Primary Connection“ (Primäre Verbindung) angezeigt.



Aktives Onboard Administrator-Modul

Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator)

Im Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator) enthalten drei Tabellen unter den Registerkarten „Status“ und „Information“ detaillierte Informationen zu Onboard Administrator.



Registerkarte „Status und Information“ (Status und Informationen)

HINWEIS: Der Zugriff auf das aktive OA-Modul über eine verbindungslokale IPv6-Adresse funktioniert möglicherweise nicht auf allen Client-System-Setups, die mehrere Netzwerkschnittstellen beinhalten.

Statusinformationen

Zeile	Beschreibung
Status (Zustand)	Der allgemeine Status des Gehäuses. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Role (Rolle)	Mögliche Werte sind „Active“ (Aktiv) oder „Standby“.
Bay Number (Einschubsnummer)	Die Nummer des physischen Einschubs, in dem das Onboard Administrator-Modul installiert ist.
Temperature (Temperatur)	Die in Celsius und Fahrenheit gemessene Temperatur des Onboard Administrator-Moduls.
Caution Threshold (Warnschwelle)	Die Temperatur, bei der das Gehäuse einen Warnstatus meldet.
Critical Threshold (Kritische Schwelle)	Die Temperatur, bei der das Gehäuse einen kritischen Status meldet.

Hardwareinformationen

Zeile	Beschreibung
Device Name (Komponentenname)	Der allgemeine beschreibende Name von Onboard Administrator.
Manufacturer (Hersteller)	Der Name des Herstellerunternehmens von Onboard Administrator.
Firmware Version (Firmwareversion)	Die Version des Firmwareimage im Onboard Administrator.
Hardware Version (Hardwareversion)	Die Version der Gehäusehardware.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen Onboard Administrator oder eines Ersatzgeräts zu verwendende Teilenummer.

Zeile	Beschreibung
Spare Part Number (Ersatzteilnummer)	Die bei der Bestellung eines zusätzlichen Onboard Administrator oder eines Ersatzgeräts zu verwendende Ersatzteilnummer.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Onboard Administrator.

Diagnostic information (Diagnoseinformationen)

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

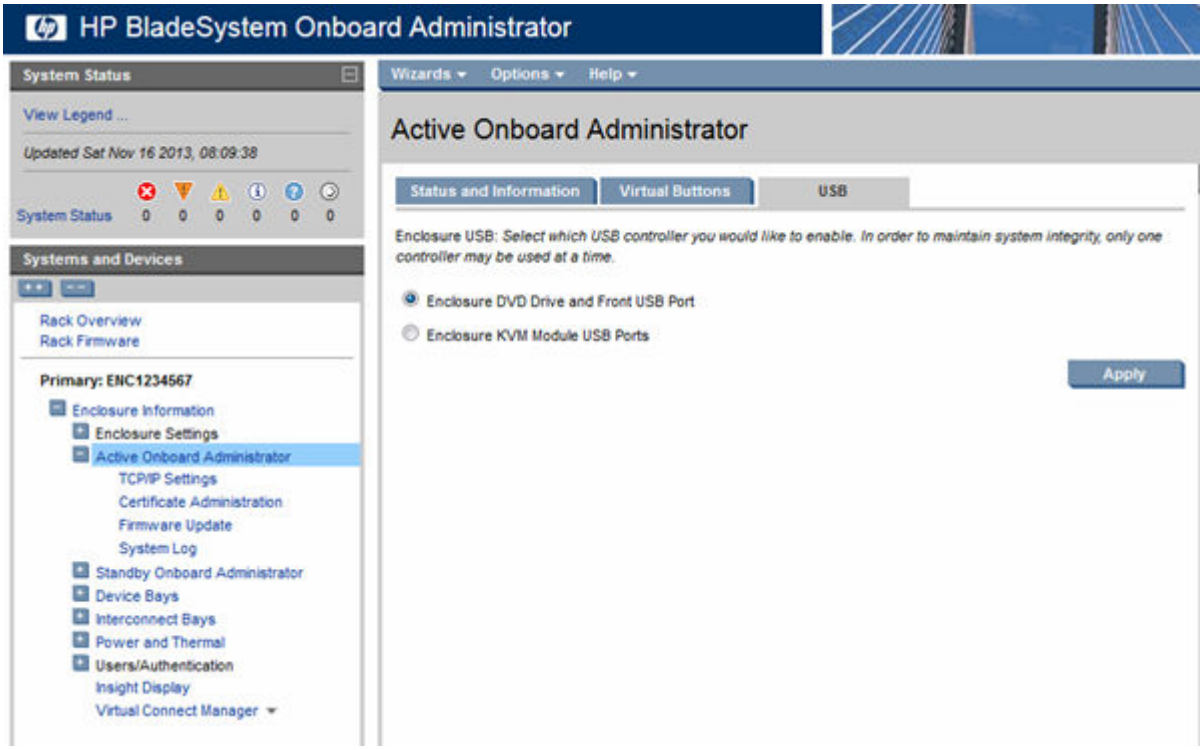
Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Diese Zeile zeigt Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen an. Diese Daten werden auch als FRU-Daten bezeichnet. Ein Komponenten-Identifikationsdaten-Fehler wird angezeigt, wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
„Firmware Mismatch“ (Unstimmige Firmware)	Der Onboard Administrator mit der niedrigsten Firmwareversion zeigt dieses Feld an, wenn zwei Onboard Administrators vorhanden sind.
OA Battery (OA-Akku)	Status des Onboard Administrator-Akkus. Mögliche Werte sind „OK“ oder „Error“ (Fehler).

Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des aktiven Onboard Administrator-Moduls

Klicken Sie auf **Reset** (Zurücksetzen), um das Onboard Administrator-Modul zurückzusetzen. Auf einem Bestätigungsbildschirm wird angefragt, ob der Vorgang wirklich durchgeführt werden soll, und darauf hingewiesen, dass der Benutzer abgemeldet und vom Onboard Administrator-Modul getrennt wird. Klicken Sie auf **OK**, um fortzufahren, oder auf **Cancel** (Abbrechen), um den Bildschirm ohne Änderung zu schließen.

Klicken Sie auf **Toggle On/Off** (Ein-/Ausschalten), um den Status der UID-LED des Onboard Administrator-Moduls zu ändern. Diese Schaltfläche erleichtert die Identifizierung eines bestimmten Onboard Administrator-Moduls, wenn mehrere vorhanden sind.

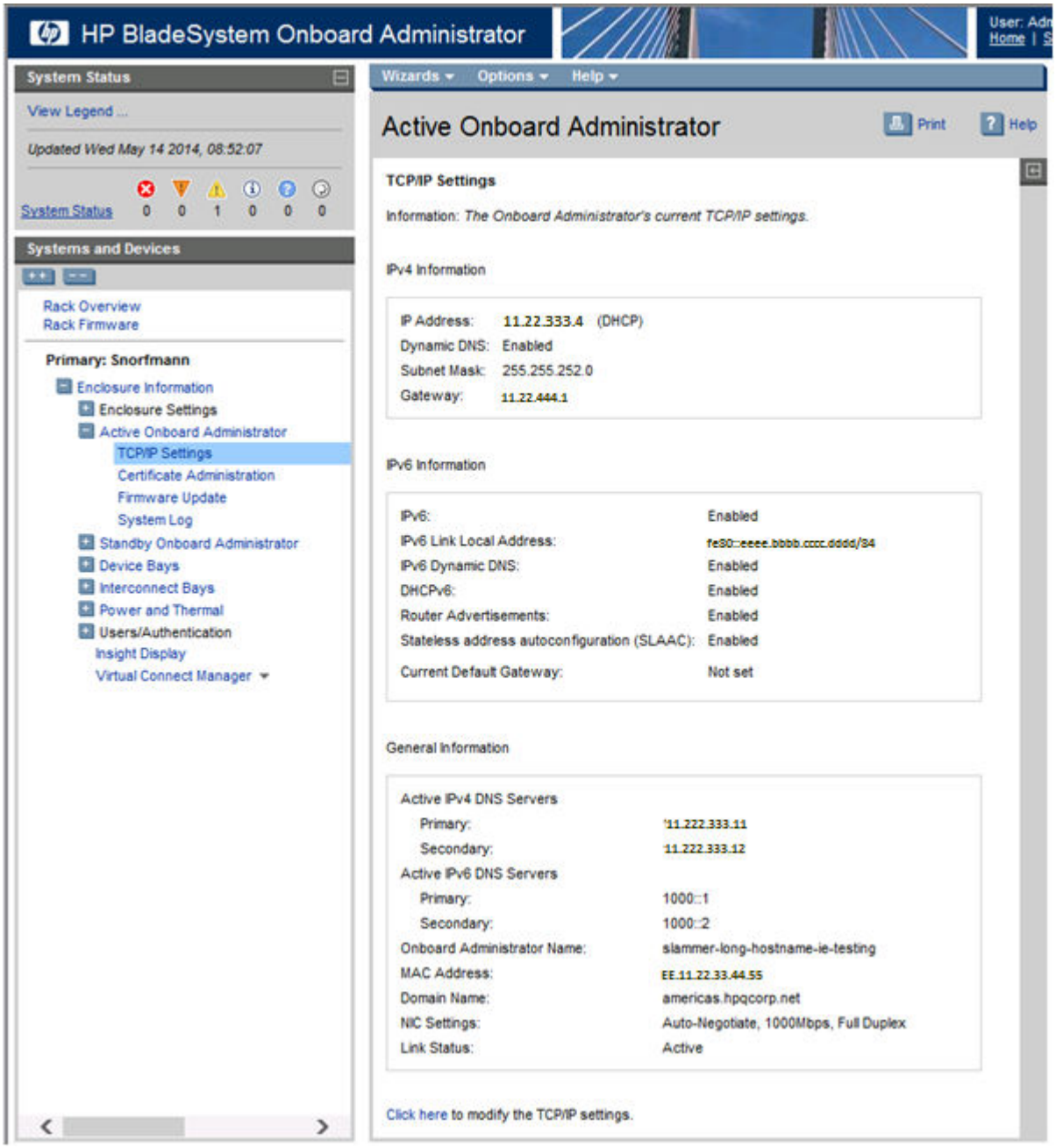
USB-Registerkarte des aktiven Onboard Administrator-Moduls



Die Registerkarte **USB** erscheint nur, wenn wenn eine frühere Version der c3000 Onboard Administrator-Karte (Hardware-Revisionsstufe A0, B0, X1 oder X3) vorhanden ist.

Bei solchen Karten kann nur jeweils ein USB-Controller verwendet werden. Auf diesem Bildschirm kann ausgewählt werden, welcher USB-Controller aktiviert werden soll: der für die USB-Ports auf dem KVM-Modul in der Rückseite des Gehäuses zuständige Controller oder der für das DVD-Laufwerk und den USB-Port an der Vorderseite des Gehäuses zuständige Controller. Bei einer Änderung des aktiven USB-Controllers wird der aktive Onboard Administrator zurückgesetzt.

Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator



Dieser Bildschirm zeigt die aktuellen Gehäuse-TCP/IP-Einstellungen für das aktive Onboard Administrator-Modul an:

- IPv4 Information (IPv4-Informationen)
- IPv6 Information (IPv6-Informationen)
- General Information (Allgemeine Informationen)

IPv4 Information (IPv4-Informationen)

Parameter	Beschreibung
IP Address (IP-Adresse)	Die IPv4-Adresse des aktiven Onboard Administrator, mit Hinweis auf den Typ der zugewiesenen IP-Adresse (statisch oder dynamisch).
Dynamic DNS (Dynamisches DNS)	Gibt an, ob „Dynamic DNS“ (Dynamisches DNS) aktiviert oder deaktiviert ist. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Datensätzen für IP-Adressen. Dies ermöglicht die Verwendung des gleichen Hostnamens über eine Zeitspanne hinweg, die für den aktiven Onboard Administrator dynamisch zugewiesene IP-Adresse kann sich jedoch ändern.
Subnet Mask (Subnetzmaske)	Die Subnetzmaske des aktiven Onboard Administrator. Die Maske bestimmt, welchem Subnetz die IP-Adresse des aktiven Onboard Administrator angehört.
Gateway	Die Gateway-Adresse des aktiven Onboard Administrator.

IPv6 Information (IPv6-Informationen)

Parameter	Beschreibung
IPv6	Gibt an, ob IPv6 auf dem aktiven Onboard Administrator-Modul aktiviert oder deaktiviert ist.
IPv6 Link Local Address (Verbindungslokale IPv6-Adresse)	Die verbindungslokale IPv6-Adresse des aktiven Onboard Administrator. Wenn IPv6 aktiviert ist, wird für den aktiven Onboard Administrator automatisch eine verbindungslokale IPv6-Adresse konfiguriert.
IPv6 Static Address 1 (Statische IPv6 Adresse 1)	IPv6-Adresse 1 des externen Onboard Administrator-NIC.
IPv6 Static Address 2 (Statische IPv6 Adresse 2)	IPv6-Adresse 2 des externen Onboard Administrator-NIC.
IPv6 Static Address 3 (Statische IPv6 Adresse 3)	IPv6-Adresse 3 des externen Onboard Administrator-NIC.
IPv6 Dynamic DNS (IPv6 - Dynamisches DNS)	Gibt an, ob „Dynamic DNS“ (Dynamisches DNS) aktiviert oder deaktiviert ist. „Dynamic DNS“ (Dynamisches DNS) aktualisiert den DNS-Server mit neuen oder geänderten Datensätzen für IP-Adressen. Dies ermöglicht die Verwendung des gleichen Hostnamens über eine Zeitspanne hinweg, die für den aktiven Onboard Administrator dynamisch zugewiesene IP-Adresse kann sich jedoch ändern.
DHCPv6	Gibt an, ob DHCPv6 auf dem aktiven Onboard Administrator aktiviert oder deaktiviert ist.
DHCPv6 Address (DHCPv6-Adresse)	Die DHCPv6-Adresse des aktiven Onboard Administrator.
Router Advertisements (Routerankündigungen)	Gibt an, ob Routerankündigungen aktiviert oder deaktiviert sind. Routerankündigungen werden für das automatische Konfigurieren von IPv6-Adressen verwendet. Wenn diese Option deaktiviert ist, werden Routerankündigungen blockiert, wodurch die SLAAC-Adresskonfiguration für alle Geräte innerhalb des Gehäuses verhindert wird.
Stateless Address Autoconfiguration (SLAAC)	Gibt an, ob SLAAC auf dem aktiven Onboard Administrator aktiviert oder deaktiviert ist. Routerankündigungen müssen aktiviert sein. Beziehen Sie sich auf die Beschreibung der Routerankündigungen.
Stateless Address Autoconfiguration (SLAAC) Address (SLAAC-Adresse)	Eine automatisch konfigurierte SLAAC-Adresse. Dem Onboard Administrator-Modul können basierend auf seiner MAC-Adresse und den über Routerankündigungen empfangenen Informationen mehrere SLAAC-Adressen zugewiesen werden.
Current Default Gateway (Aktuelles Standard-Gateway)	Gibt die IPv6-Adresse des Standard-Gateways an, das derzeit vom aktiven Onboard Administrator verwendet wird. Bei dem aktuellen Standardgateway kann es sich um

Parameter	Beschreibung
	das statische Standardgateway oder um ein über Routerankündigungen konfiguriertes Gateway handeln. Wenn die IPv6-Gatewaykonfiguration über Routerankündigungen bereitgestellt wird, wird die statische IPv6-Gateway-Einstellung durch deren Gatewaykonfiguration übersteuert.
Static Default Gateway (Statisches Standard-Gateway)	Gibt die statische IPv6-Adresse des IPv6-Standard-Gateways an. Sie wird nur angezeigt, wenn sie konfiguriert ist.
Static Route 1 (Statischer Verbindungsweg 1)	Die Adresse des externen Netzwerks oder Knotens, die Onboard Administrator über ein verknüpftes Gateway des statischen Verbindungswegs erreichen kann.
Gateway (Static Route 1) (Gateway (Statischer Verbindungsweg 1))	Die Adresse des Gateways, über das Onboard Administrator das Ziel des statischen Verbindungsweges 1 erreicht.
Static Route 2 (Statischer Verbindungsweg 2)	Ein zweiter statischer IPv6-Verbindungsweg.
Gateway (Static Route 2) (Gateway (Statischer Verbindungsweg 2))	Die Adresse des Gateways, über das Onboard Administrator das Ziel des statischen Verbindungsweges 2 erreicht.
Static Route 3 (Statischer Verbindungsweg 3)	Ein dritter statischer IPv6-Verbindungsweg.
Gateway (Static Route 3) (Gateway (Statischer Verbindungsweg 3))	Die Adresse des Gateways, über das Onboard Administrator das Ziel des statischen Verbindungsweges 3 erreicht.

General Information (Allgemeine Informationen)

Parameter	Beschreibung
Active IPv4 DNS Servers (Aktive IPv4 DNS-Server)	Listet die konfigurierten IPv4 DNS-Server auf, die auf dem aktiven Onboard Administrator-Modul* aktiv sind.
Primary (Primär)	Die IP-Adresse des ersten IPv4 DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, wird `Not set` (Nicht festgelegt) angezeigt.
Secondary (Sekundär)	Die IP-Adresse des zweiten IPv4 DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, wird `Not set` (Nicht festgelegt) angezeigt.
Active IPv6 DNS Servers (Aktive IPv6 DNS-Server)	Listet die konfigurierten IPv6 DNS-Server auf, die auf dem aktiven Onboard Administrator-Modul* aktiv sind.
Primary (Primär)	IP-Adresse des ersten IPv6 DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, wird `Not set` (Nicht festgelegt) angezeigt.
Secondary (Sekundär)	Die IP-Adresse des zweiten IPv6 DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, wird `Not set` (Nicht festgelegt) angezeigt.
Tertiary (Tertiär)	Die IP-Adresse des dritten IPv6 DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, werden dieser Parameter und die Adresse nicht angezeigt.
Quaternary (Quartär)	Die IP-Adresse des vierten DNS-Servers, der von dem aktiven Onboard Administrator-Modul verwendet wird. Wenn sie nicht konfiguriert ist, werden dieser Parameter und die Adresse nicht angezeigt.
Onboard Administrator Name	Der Name (DNS-Hostname), der für das aktive Onboard Administrator-Modul verwendet wird.

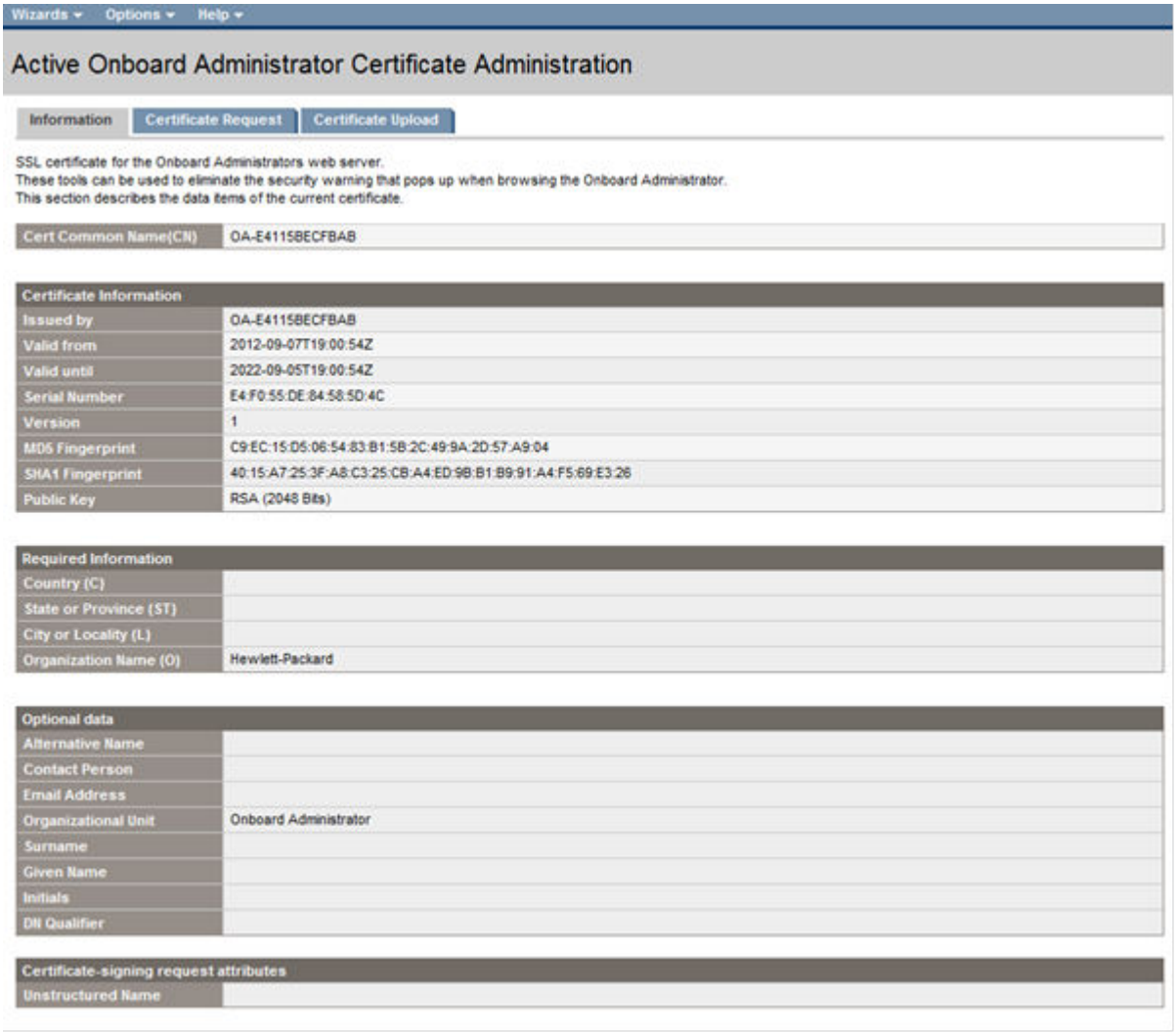
Parameter	Beschreibung
VLAN ID (Name)	Die eindeutige Nummer, durch die das VLAN identifiziert wird. Wird nur angezeigt, wenn der VLAN-Modus aktiviert ist.
MAC Address (MAC-Adresse)	Die MAC-Adresse des aktiven Onboard Administrator.
Domain Name (Domänenname)	Der Name der Domäne für den aktiven Onboard Administrator.
NIC Settings (NIC-Einstellungen)	Die NIC-Einstellungen für den aktiven Onboard Administrator, wie z. B. automatische Aushandlung, Duplexmodus und Geschwindigkeit.
Link Status (Verbindungszustand)	Gibt an, ob die NIC aktiv mit dem Netzwerk verbunden ist.

* Die Reihenfolge, in der Onboard Administrator DNS-Server verwendet, wird auf der Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) (Registerkarte „IPv4-Einstellungen“ auf Seite 126) und auf der Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) (Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf Seite 129) beschrieben.

Um die TCP/IP-Einstellungen zu ändern, wählen Sie **Click here** (Hier klicken).

Informationen zu den TCP/IP-Einstellungen, die von Ihnen geändert werden können, finden Sie auf der Registerkarte „Enclosure TCP/IP IPv4 Settings“ (TCP/IP-IPv4-Einstellungen des Gehäuses) (Registerkarte „IPv4-Einstellungen“ auf Seite 126) und auf der Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) (Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf Seite 129).

Registerkarte „Certificate Administration Information“ (Zertifikatsverwaltungsinformationen)



Registerkarte „Information“

Dieser Bildschirm zeigt detaillierte Informationen zu dem derzeit von Onboard Administrator verwendeten SSL-Zertifikat an. Ein SSL-Zertifikat dient zur Bescheinigung der Identität von Onboard Administrator und wird von dem zugrunde liegenden HTTP-Server zum Aufbau einer sicheren (verschlüsselten) Kommunikationsverbindung mit dem Client-Web-Browser vorgeschrieben.

Beim ersten Starten erstellt Onboard Administrator ein 10 Jahre lang gültiges, selbstsigniertes SSL-Standardzertifikat, das auf den Namen des Onboard Administrator-Moduls ausgestellt ist. Da dieses Standardzertifikat selbstsigniert ist, wird das Feld „Issued by“ (Ausgestellt von) auf den gleichen Namen eingestellt.

Statusinformationen

Zeile	Beschreibung
Cert Common Name (Allgemeine Name des Zertifikats)	Der allgemeine Name des Zertifikats.

Certificate Information (Informationen zum Zertifikat)

Zeile	Beschreibung
Issued by (Ausgestellt von)	Die Zertifizierungsstelle, die das Zertifikat ausgestellt hat.
Valid from (Gültig ab)	Das Datum, ab dem das Zertifikat gültig ist.
Valid until (Gültig bis)	Das Datum, an dem das Zertifikat abläuft.
Serial Number (Seriennummer)	Die dem Zertifikat von der Zertifizierungsstelle zugewiesene Seriennummer.
Version	Die Versionsnummer des aktuellen Zertifikats.
MD5 Fingerprint (MD5-Fingerabdruck)	Dieses im Zertifikat eingebettete Feld dient der Echtheitsprüfung.
SHA1 Fingerprint (SHA1-Fingerabdruck)	Dieses im Zertifikat eingebettete Feld dient der Echtheitsprüfung.
Public Key (Öffentlicher Schlüssel)	Der Name des öffentlichen Schlüssels.

Benötigte Informationen

Zeile	Beschreibung
Country (C) (Land):	Ein zweistelliger Landescode, durch den das Land identifiziert wird, in dem sich Onboard Administrator befindet.
State or Province (ST) (Bundesstaat oder Provinz):	Der Bundesstaat oder die Provinz, in der sich Onboard Administrator befindet.
City or Locality (L) (Stadt oder Ort):	Die Stadt oder der Ort, in der bzw. an dem sich Onboard Administrator befindet.
Organization Name (O) (Name der Organisation):	Die Firma, in deren Besitz sich dieser Onboard Administrator befindet.

Optional data (Optionale Daten)

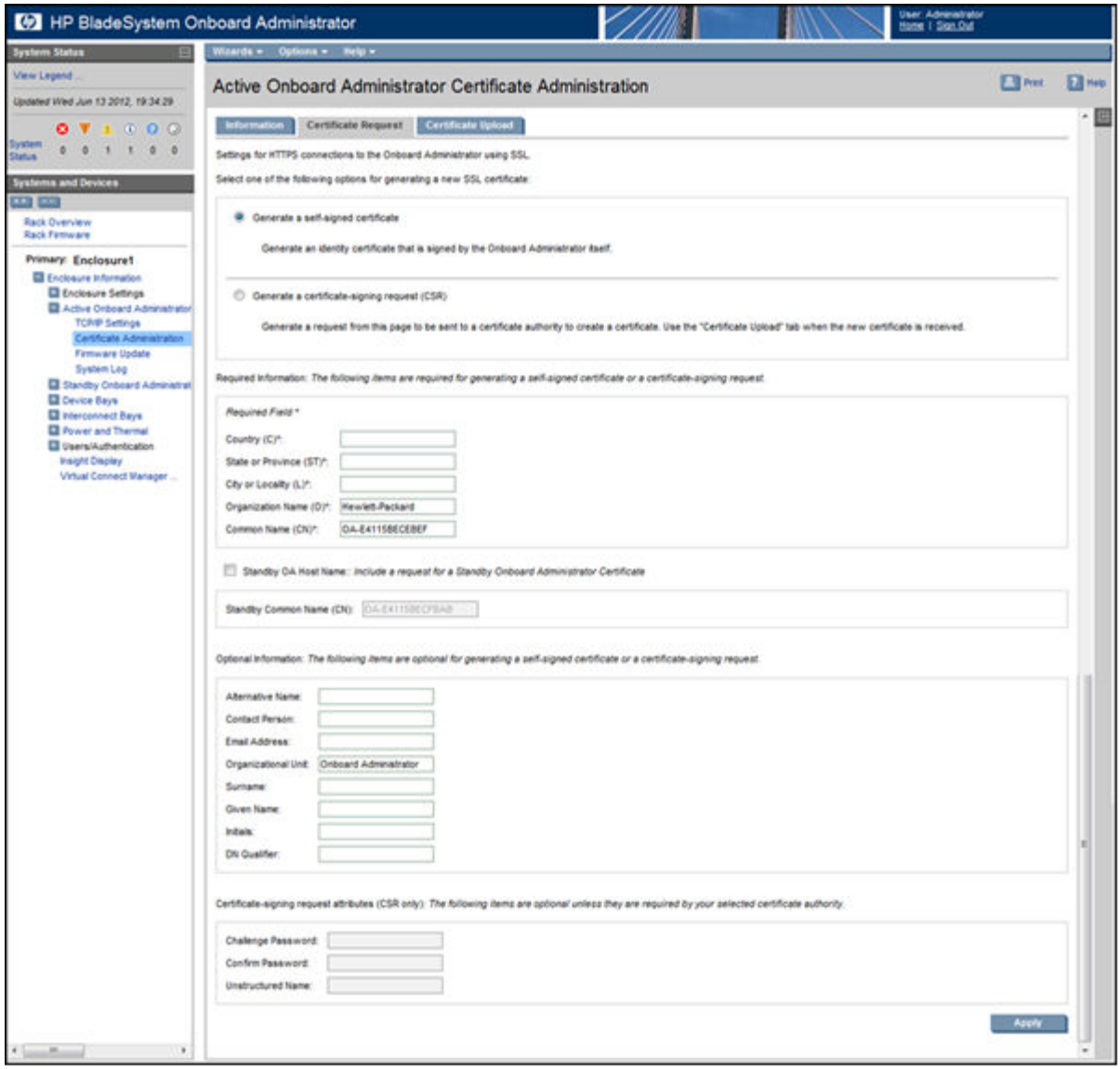
Zeile	Beschreibung
Alternative Name (Alternativer Name)	Ein alternativer Name für den Onboard Administrator.
Contact Person (Kontaktperson)	Die für Onboard Administrator verantwortliche Person.
Email Address (E-Mail-Adresse)	Die E-Mail-Adresse der für Onboard Administrator verantwortlichen Person.
Organizational Unit (Organisationseinheit)	Die Einheit innerhalb der Firma oder Organisation, in deren Besitz sich Onboard Administrator befindet.
Surname (Vorname)	Der Vorname der für Onboard Administrator verantwortlichen Person.
Given Name (Nachname)	Der Nachname der für Onboard Administrator verantwortlichen Person.
Initials (Initialen)	Die Initialen der für Onboard Administrator verantwortlichen Person.
DN Qualifier (DN-Kennzeichner)	Der eindeutige Namenskennzeichner von Onboard Administrator.

Certificate-signing request attributes (Zertifikatssignierungs-Anforderungsattribute)

Zeile	Beschreibung
Unstructured Name (Unstrukturierter Name)	Dies sind zusätzliche Informationen.

Registerkarte „Certificate Request“ (Zertifikat-Anforderung)

Auf der Registerkarte „Certificate Request“ (Zertifikat-Anforderung) können Sie die Informationen eingeben, die zum Erstellen eines selbstsignierten Zertifikats oder einer genormten Zertifikatssignierungsanforderung an eine Zertifizierungsstelle erforderlich sind.



Benötigte Informationen

Feld	Mögliche Werte	Beschreibung
Country (C) (Land)	Muss 1 bis 2 Zeichen lang sein. Zulässige Zeichen	Ein gültiger Landescode, durch den das Land identifiziert wird, in dem sich Onboard Administrator befindet.

Feld	Mögliche Werte	Beschreibung
	sind alle alphanumerischen Zeichen, ein Leerzeichen und die folgenden Satzzeichen: : ' ( ) + , - . / : = ?	
State or Province (ST) (Bundesstaat oder Provinz)	Muss 1 bis 30 Zeichen lang sein.	Der Bundesstaat oder die Provinz, in der sich Onboard Administrator befindet.
City or Locality (L) (Stadt oder Ort)	Muss 1 bis 50 Zeichen lang sein.	Die Stadt oder der Ort, in der bzw. an dem sich Onboard Administrator befindet.
Organization Name (O) (Name der Organisation)	Muss 1 bis 60 Zeichen lang sein.	Die Organisation, in deren Besitz sich dieser Onboard Administrator befindet. Wenn anhand dieser Informationen eine Zertifikatssignierungsanforderung erstellt wird, kann die ausstellende Zertifizierungsstelle prüfen, ob die das Zertifikat anfordernde Organisation gesetzlich dazu berechtigt ist, sich als Besitzer des betreffenden Firmennamens oder der betreffenden Organisation auszugeben.
Common Name (CN) (Allgemeiner Name)	Muss 1 bis 60 Zeichen lang sein. Damit keine Sicherheitswarnungen ausgegeben werden, muss der Wert dieses Feldes genau dem Hostnamen entsprechen, der dem Web-Browser bekannt ist. Der Browser vergleicht den Hostnamen in der aufgelösten Webadresse mit dem im Zertifikat angegebenen Namen. Lautet die Webadresse im Adressfeld beispielsweise https://oa-001635.xyz.com, muss der Wert oa-001635.xyz.com lauten.	Der im Web-Adressfeld des Browsers angezeigte Onboard Administrator-Name. Dieses Zertifikatattribut wird in der Regel als der geläufige Name bezeichnet.

Wählen Sie **Standby OA Host Name** (Hostname des OA-Standby-Moduls), wenn Sie eine Zertifikatanforderung für ein Onboard Administrator Standby-Modul einschließen möchten. Geben Sie die Informationen in das Feld **Standby Common Name (CN)** (Allgemeiner Name des Standby-Moduls (CN)) ein. Der Eintrag muss 1 bis 60 Zeichen lang sein. Diese Option wird nur angezeigt, wenn im Gehäuse ein Onboard Administrator Standby-Modul vorhanden ist.

Optional Information (Optionale Informationen)

Feld	Mögliche Werte	Beschreibung
Alternative Name (Alternativer Name)	Muss 0 bis 511 Zeichen lang sein.	Ein alternativer Name für den Onboard Administrator. Der Name wird zum Erstellen des Erweiterungsattributs „X509v3 Subject Alternative Name“ verwendet. Das Feld muss entweder leer sein oder eine Liste von durch Kommas getrennter Schlüsselwort:Wert-Paare enthalten. Zu den gültigen Schlüsselwort:Wert-Einträgen gehören IP:<IP-Adresse> und DNS:<Domänenname>.

Feld	Mögliche Werte	Beschreibung
Contact Person (Kontaktperson)	Muss 0 bis 60 Zeichen lang sein.	Die für Onboard Administrator verantwortliche Person.
Email Address (E-Mail-Adresse)	Muss 0 bis 60 Zeichen lang sein.	Die E-Mail-Adresse der für Onboard Administrator verantwortlichen Kontaktperson.
Organizational Unit (Organisationseinheit)	Muss 0 bis 60 Zeichen lang sein.	Die Einheit innerhalb der Firma oder Organisation, in deren Besitz sich Onboard Administrator befindet.
Surname (Vorname)	Muss 0 bis 60 Zeichen lang sein.	Der Vorname der für Onboard Administrator verantwortlichen Person.
Given Name (Nachname)	Muss 0 bis 60 Zeichen lang sein.	Der Nachname der für Onboard Administrator verantwortlichen Person.
Initials (Initialen)	Muss 0 bis 20 Zeichen lang sein.	Die Initialen der für Onboard Administrator verantwortlichen Person.
DN Qualifier (DN-Kennzeichner)	Muss 0 bis 60 Zeichen lang sein. Zulässige Zeichen sind alle alphanumerischen Zeichen, das Leerzeichen sowie die folgenden Satzzeichen: ' ( ) + , - . / : = ?	Der eindeutige Namenskennzeichner von Onboard Administrator.

Certificate-signing request attributes (Zertifikatssignierungs-Anforderungsattribute)

Feld	Mögliche Werte	Beschreibung
Challenge Password (Kennwort)	Muss 0 bis 30 Zeichen lang sein.	Das Kennwort der Zertifikatssignierungsanforderung.
Confirm Password (Kennwortbestätigung)	Muss 0 bis 30 Zeichen lang sein.	Dient zur Bestätigung des Kennworts.
Unstructured Name (Unstrukturierter Name)	Muss 0 bis 60 Zeichen lang sein.	Dieses Feld ist für Zusatzinformationen bestimmt, beispielsweise für einen Onboard Administrator zugewiesenen unstrukturierten Namen.

Klicken Sie auf **Apply** (Übernehmen). Es wird ein selbstsigniertes Zertifikat bzw. eine genormte Zertifikatssignierungsanforderung erstellt.

Standardized certificate-signing request (Genormte Zertifikatssignierungsanforderung)

Dieser Bildschirm zeigt eine von Onboard Administrator erstellte genormte Zertifikatssignierungsanforderung an. Der Inhalt der Anforderung im Textfeld kann zwecks Signierung an eine Zertifizierungsstelle Ihrer Wahl gesendet werden. Das von der Zertifizierungsstelle zurückgesandte signierte Zertifikat kann auf der Registerkarte „Certificate Upload“ (Zertifikat-Upload) hochgeladen werden.

War für Onboard Administrator eine statische IP-Adresse konfiguriert, als diese Zertifikatanforderung erstellt wurde, wird die Anforderung an die statische IP-Adresse ausgegeben. Andernfalls wird sie an den dynamischen DNS-Namen von Onboard Administrator ausgegeben. Das Zertifikat fordert standardmäßig eine Gültigkeitsdauer von 10 Jahren an (dieser Wert kann derzeit nicht konfiguriert werden).

Beim Senden der Anforderung an die Zertifizierungsstelle müssen Sie auf Folgendes achten:

1. Verwenden Sie die Onboard Administrator-Internet-Adresse (URL) für den Server.
2. Fordern Sie die Erzeugung des Zertifikats im RAW-Format an.
3. Schließen Sie die Zertifikatzeilen „Begin“ und „End“ ein.

Registerkarte „Certificate Upload“ (Zertifikat-Upload)

Um Zertifikate zur Verwendung auf dem HP BladeSystem Onboard Administrator hochzuladen, muss der Benutzer über das Administrator-Konto angemeldet sein.

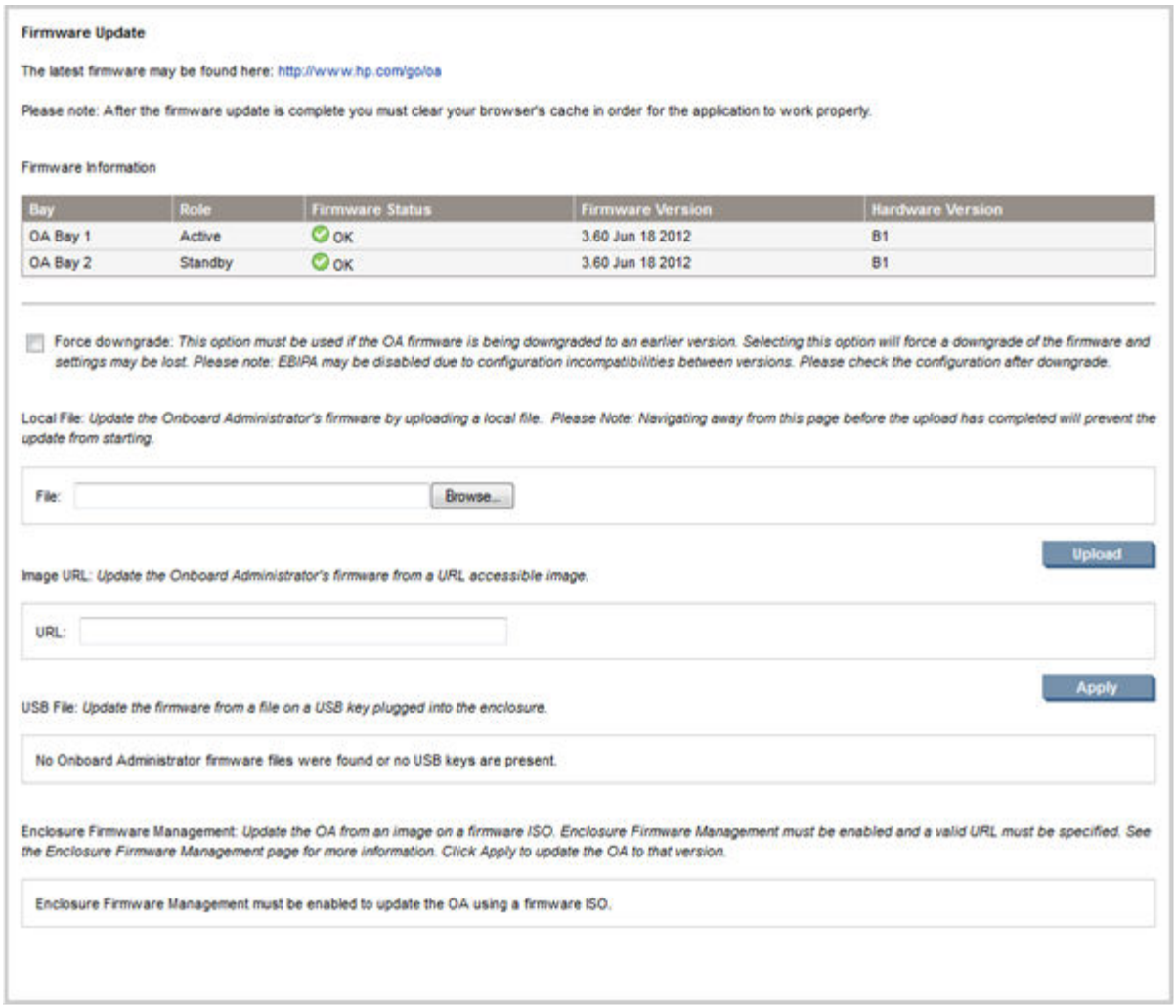
Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Das hochzuladende Zertifikat muss sich auf eine Zertifikatsanforderung für den betreffenden Onboard Administrator zurückführen lassen, die an eine Zertifizierungsstelle gesendet und von ihr signiert wurde. Andernfalls stimmt das Zertifikat nicht mit den privaten Schlüsseln überein, die zur Erstellung der Zertifikatsanforderung verwendet wurden, und wird zurückgewiesen. Wurde die Onboard Administrator-Domäne zerstört oder neu importiert, müssen die Schritte zur Erstellung einer Zertifikatanforderung ebenfalls wiederholt werden. Es wird von einer Zertifizierungsstelle neu zugewiesen, da die privaten Schlüssel zusammen mit der Onboard Administrator-Domäne zerstört und neu erstellt werden.

Nachdem das neue Zertifikat von Onboard Administrator akzeptiert und erfolgreich installiert wurde, werden Sie automatisch abgemeldet. Der HTTP-Server muss neu gestartet werden, damit das neue Zertifikat wirksam wird.

Firmware-Aktualisierung


Firmware Update
The latest firmware may be found here: http://www.hp.com/go/oa
Please note: After the firmware update is complete you must clear your browser's cache in order for the application to work properly.
Firmware Information
Bay
Role
Firmware Status
Firmware Version
Hardware Version
OA Bay 1
Active
OK
3.60 Jun 18 2012
B1
OA Bay 2
Standby
OK
3.60 Jun 18 2012
B1
Force downgrade: This option must be used if the OA firmware is being downgraded to an earlier version. Selecting this option will force a downgrade of the firmware and settings may be lost. Please note: EBIPA may be disabled due to configuration incompatibilities between versions. Please check the configuration after downgrade.
Local File: Update the Onboard Administrator's firmware by uploading a local file. Please Note: Navigating away from this page before the upload has completed will prevent the update from starting.
File:
Browse...
Upload
Image URL: Update the Onboard Administrator's firmware from a URL accessible image.
URL:
Apply
USB File: Update the firmware from a file on a USB key plugged into the enclosure.
No Onboard Administrator firmware files were found or no USB keys are present.
Enclosure Firmware Management: Update the OA from an image on a firmware ISO. Enclosure Firmware Management must be enabled and a valid URL must be specified. See the Enclosure Firmware Management page for more information. Click Apply to update the OA to that version.
Enclosure Firmware Management must be enabled to update the OA using a firmware ISO.

⚠ ACHTUNG: Trennen Sie nicht die Verbindung der Onboard Administrator-Module während einer laufenden Firmwareaktualisierung. Durch Trennen dieser Module könnte der Onboard Administrator inoperabel werden.

Auf diesem Bildschirm wird die aktuelle Firmwareversion angezeigt, die auf dem aktiven Onboard Administrator-Modul und auf dem Onboard Administrator-Standby-Modul installiert ist. Die aktuelle Hardwareversion von Onboard Administrator wird ebenfalls auf diesem Bildschirm angegeben.

Synchronize firmware (Firmware synchronisieren)

Um die Firmware auf dem aktiven Onboard Administrator und auf dem Standby-Onboard Administrator auf die gleiche Firmwareversion zu synchronisieren, klicken Sie auf **Synchronize Firmware** (Firmware synchronisieren). Es wird ein Firmware-Image vom Flash-Inhalt des Onboard Administrator mit der neuesten Firmwareversion erstellt und zum Onboard Administrator mit der ältesten Firmwareversion geflasht. Nachdem die Firmware geflasht wurde, wird der aktualisierte Onboard Administrator neu gestartet.

So verwenden Sie die Funktion „Synchronize Firmware“ (Firmware synchronisieren):

- Auf beiden Onboard Administrator-Modulen muss Firmwareversion 2.10 oder höher ausgeführt werden.
- Wenn auf dem aktiven Onboard Administrator-Modul VLAN aktiviert ist, muss die Firmware des Standby-Onboard Administrator-Moduls mit der VLAN-Funktion kompatibel sein. Wenn das Standby-Onboard Administrator-Modul über eine ältere Version verfügt, die VLAN nicht unterstützt, dann muss das Standby-Onboard Administrator-Modul entfernt und die Firmware über ein anderes Gehäuse auf eine kompatible Version aktualisiert werden.

Herabstufen der Firmware

Force Downgrade (Herabstufung erzwingen) – Mit dieser Option können Sie die Herabstufung des Onboard Administrator auf eine frühere Version erzwingen. Bei Auswahl dieser Option wird ein Herabstufung der Firmware erzwungen. Aktuelle Einstellungen, die bei der früheren Version nicht anwendbar sind, gehen möglicherweise verloren. Wenn sich der Onboard Administrator im VC-Modus befindet und IPv6 aktiviert ist, gibt der Virtual Connect Manager möglicherweise die mindestens erwartete Firmwareversion für den Onboard Administrator an. Wenn diese Situation eintritt, wird durch die Deaktivierung der Onboard Administrator-IPv6-Kommunikation vor dem Herabstufungsversuch die Kompatibilität von VC mit älteren Onboard Administrator-Versionen gewährleistet.

HINWEIS: Diese Funktion ist im FIPS-Modus ON/DEBUG deaktiviert.

Update firmware

ACHTUNG: Im FIPS-Modus ON/DEBUG werden bei einem Upgrade auf die aktuelle Version von Onboard Administrator von einer Version vor 4.40 die ersten 21 erstellten lokalen Benutzerkonten beibehalten, einschließlich aller reservierten Konten wie z. B. Administrator oder Virtual Connect-Benutzer. Die restlichen Benutzerkonten werden gelöscht.

Local File (Lokale Datei): Um die Firmware auf dem aktiven Onboard Administrator-Modul über eine lokale Datei zu aktualisieren, suchen Sie nach der Firmware-Image-Datei oder geben Sie den Pfad der Firmware-Image-Datei in das Textfeld ein. Die maximale Anzahl von Zeichen im Dateipfad ist 256. Klicken Sie auf **Upload** (Hochladen).

Image URL (Image-URL): So aktualisieren Sie die Firmware auf dem aktiven Onboard Administrator-Modul über eine Datei, die sich auf einem Webserver befindet:

1. Geben Sie einen http://-Pfad zur Firmware-Image-Datei ein. Unterstützte Protokolle sind HTTP, FTP und TFTP. Der URL besitzt das folgende Format: Protokoll://Host/Pfad/Dateiname. Die URL-Syntax der IPv6-Adresse lautet:

   Protokoll://[IPv6-Adresse]/Pfad/Datei

   Die maximale Länge der URL beträgt 511 Zeichen.

   Sollte Ihr FTP-Server keine anonymen Anmeldungen unterstützen, können Sie innerhalb des URL in folgendem Format einen Benutzernamen und ein Kennwort angeben: ftp://Benutzername:Kennwort@Host/Pfad/Dateiname.

   HINWEIS: Geben Sie bei Einsatz des FTP-Protokolls den URL-Pfad des Image in diesem Format ein. Geben Sie vor dem Teil „Host/Pfad/Dateiname“ des URL einen doppelten Schrägstrich (//) an: ftp://Benutzer:Kennwort@//Host/Pfad/Dateiname.

HINWEIS: Aufgrund des ab Onboard Administrator v4.11 geänderten Verhaltens suchen einige FTP-Server bei Eingabe eines einzelnen Schrägstrichs (/) anstatt eines doppelten Schrägstrichs in Ihrem Basisverzeichnis als relativem Stammpfad (/Basis/Benutzer/Pfad/Dateiname) nach der Image-Datei. Durch Angabe der empfohlenen doppelten Schrägstriche wird sichergestellt, dass der FTP-Server im absoluten Pfad (/Pfad/Dateiname) nach dem Image sucht.

2. Geben Sie den URL ein, und klicken Sie dann auf **Apply** (Übernehmen).
3. Nach dem Klicken auf **Upload** (Hochladen) oder **Apply** (Übernehmen) wird ein Fenster angezeigt, das den Fortschritt beim Herunterladen der Firmware angezeigt. Nach dem das Herunterladen abgeschlossen wurde, werden Sie vom Onboard Administrator abgemeldet und müssen sich wieder neu anmelden.

USB File (USB-Datei): Um auf dem aktiven Onboard Administrator Firmware aus einem Abbild zu aktualisieren, das sich auf einem USB-Schlüssel befindet, wählen Sie eine Datei aus dem Menü aus und klicken Sie anschließend auf **Apply** (Übernehmen). Dieses Feld wird nur angezeigt, wenn im USB-Port des aktiven Onboard Administrator ein USB-Schlüssel erkannt wird und sich auf diesem USB-Schlüssel Firmwareabbilder befinden. Die maximale unterstützte USB-Schlüsselgröße ist 4 GB.

Beim Einleiten der Firmwareaktualisierung wird ein Zeitgeber angezeigt, während anderen Benutzern in einem Dialogfeld mitgeteilt wird, dass das Gehäuse ausgeschaltet und neu gestartet wird. Nachdem das Gehäuse neu gestartet wurde, müssen Sie sich erneut anmelden.

Wenn zwei Gehäuse angeschlossen sind, wird durch die Firmwareaktualisierung zuerst das Onboard Administrator Standby-Modul und anschließend das primäre Onboard Administrator-Modul aktualisiert. Wenn unmittelbar nach einer Firmware-Aktualisierung keine Verbindung hergestellt werden kann, warten Sie 30 Sekunden, bis das Gehäuse im Netzwerk zur Verfügung steht.

Enclosure Firmware Management

Sie können den Onboard Administrator über ein Firmware-ISO-Abbild aktualisieren. Die Funktion „Enclosure Firmware Management“ muss aktiviert sein und in den Einstellungen muss eine gültige URL angegeben werden. Weitere Informationen finden Sie unter „Enclosure Firmware Management“ (Enclosure Firmware Management auf Seite 197).

Um Onboard Administrator zu aktualisieren, klicken Sie auf **Apply** (Übernehmen).

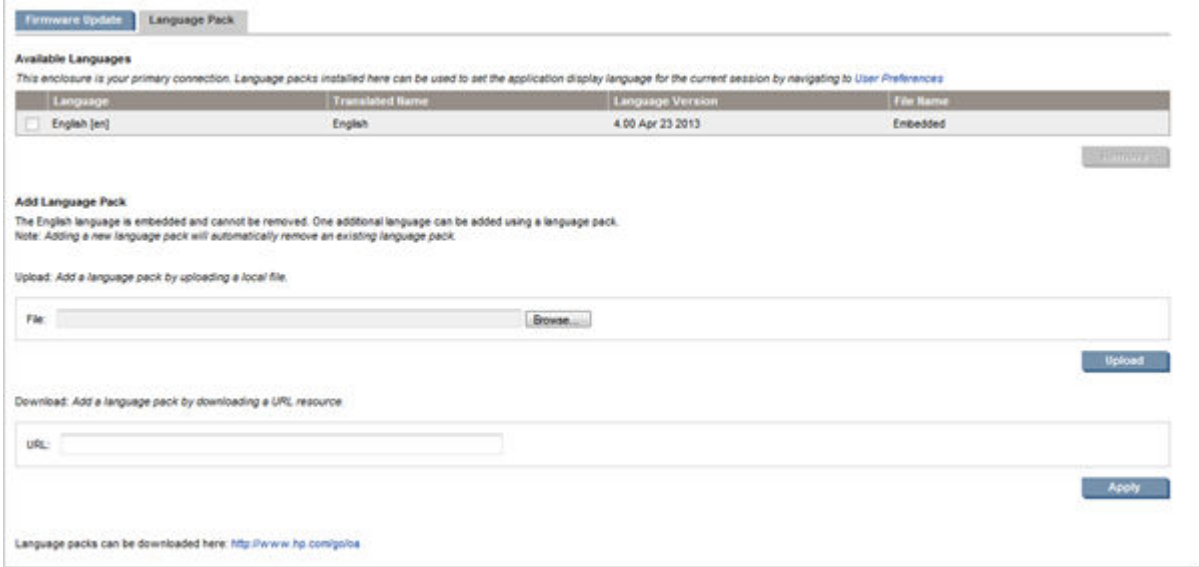
Installieren einer vorherigen Version

Wenn Sie eine vorherige Version der Firmware installieren möchten, markieren Sie das Kontrollkästchen **Force downgrade** (Downgrade erzwingen) im Bildschirmbereich „Firmware Information“ (Firmwareinformationen). Suchen Sie lokal oder durch Eingabe einer URL in den Eingabefeldern nach der Firmwaredatei. Wenn Sie einen Downgrade der Onboard Administrator-Firmware auf 2.31 oder niedriger durchführen, verlieren Sie bis auf die ersten fünf Gruppen alle Verzeichnisgruppen. Onboard Administrator-Versionen höher als 2.31 unterstützen 30 Gruppen, während frühere Versionen nur fünf Gruppen unterstützen. Nach den ersten fünf Gruppen werden weitere Verzeichnisbenutzer ausgeschlossen.

Wenn Sie versuchen, bei aktiviertem IPv6 eine Herabstufung auf eine vorherige Version durchzuführen, schreibt VC eine Mindestversion der Onboard Administrator-Firmware vor. Um mit der Herabstufung fortzufahren, deaktivieren Sie IPv6 und wiederholen den Vorgang.

Die neueste Firmware für Onboard Administrator ist von der HP Onboard Administrator-Website (http://www.hp.com/go/oa) verfügbar.

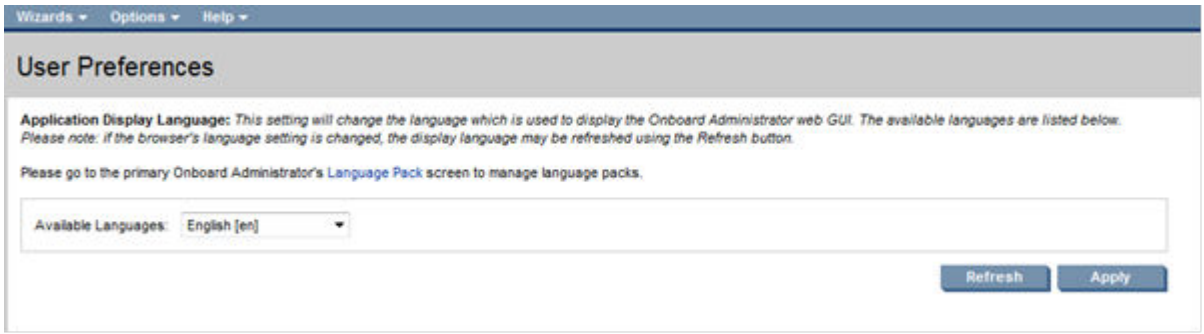
Registerkarte „Language Pack“ (Sprachpaket)


Firmware Update
Language Pack
Available Languages
This enclosure is your primary connection. Language packs installed here can be used to set the application display language for the current session by navigating to User Preferences
Language
Translated Name
Language Version
File Name
English [en]
English
4.00 Apr 23 2013
Embedded
Remove
Add Language Pack
The English language is embedded and cannot be removed. One additional language can be added using a language pack.
Note: Adding a new language pack will automatically remove an existing language pack.
Upload: Add a language pack by uploading a local file.
File:
Browse...
Upload
Download: Add a language pack by downloading a URL resource.
URL:
Apply
Language packs can be downloaded here: http://www.hp.com/go/oa

In diesem Bildschirm wird die Liste der installierten Sprachpakete angezeigt. Die englische Sprache ist eingebettet und kann nicht entfernt werden. Mittels eines Sprachpakets kann nur eine zusätzliche Sprache hinzugefügt werden. Durch das Hinzufügen eines neuen Sprachpakets wird ein vorhandenes Sprachpaket automatisch entfernt. Um ein vorhandenes Sprachpaket zu entfernen, markieren Sie das Kontrollkästchen, und klicken Sie auf **Remove** (Entfernen).

Sie haben zwei Optionen für das Hinzufügen eines Sprachpakets:

- **Upload** (Hochladen): Zum Hinzufügen eines Sprachpakets über eine lokale Datei suchen Sie nach der Sprachpaketdatei, oder geben Sie den Pfad der Sprachpaketdatei in das Textfeld ein. Die maximale Anzahl von Zeichen im Dateipfad ist 256. Klicken Sie auf **Upload** (Hochladen).
- **Download** (Herunterladen) – Zum Hinzufügen eines Sprachpakets über eine Datei auf einem Webserver geben Sie einen http://-Pfad zur Firmware-Image-Datei ein. Die maximale Anzahl von Zeichen im Dateipfad ist 255. Unterstützte Protokolle sind HTTP, FTP und TFTP. Der URL besitzt das folgende Format: Protokoll://Host/Pfad/Dateiname. Geben Sie den URL ein, und klicken Sie anschließend auf **Apply** (Übernehmen). Nachdem Sie auf „Upload“ (Hochladen) oder „Apply“ (Übernehmen) geklickt haben, wird in einem Fenster der Fortschritt des Firmware-Downloads angezeigt. Nach Abschluss des Downloads wird in einem Popup-Fenster das hinzugefügte Sprachpaket angezeigt.


Wizards
Options
Help
User Preferences
Application Display Language: This setting will change the language which is used to display the Onboard Administrator web GUI. The available languages are listed below.
Please note: if the browser's language setting is changed, the display language may be refreshed using the Refresh button.
Please go to the primary Onboard Administrator's Language Pack screen to manage language packs.
Available Languages:
English [en]
Refresh
Apply

Nach der Installation eines Sprachpakets können Sie die Sprache mittels der Spracheinstellungsoption des aktuellen Browsers auf der Onboard Administrator-GUI (vorzugsweise) oder mittels der Optionen unter „User Preferences“ (Benutzereinstellungen) im Onboard Administrator anzeigen:

- Um für die Spracheinstellungen die Einstellungen des Browsers zu verwenden, fügen Sie die gewünschte Sprache am Anfang der Browserliste der bevorzugten Sprachen hinzu und wählen Sie dann auf dem Onboard Administrator-Bildschirm „User Preferences“ (Benutzereinstellungen) (Benutzereinstellungen auf Seite 56) die Option „Use browser settings“ (Browser-Einstellungen verwenden) aus. Diese Methode wird bevorzugt, da die Einstellung für alle nachfolgenden Onboard Administrator-GUI-Sitzungen gilt, die von diesem Browser Gebrauch machen. Die Einstellung gilt auch für Sitzungen mit anderen Onboard Administrator-Modulen, sofern auf den anderen Onboard Administrator-GUIs die gleiche Sprache installiert ist und für die Einstellung „User Preferences“ (Benutzereinstellungen) die Standardeinstellung „Use browser settings“ (Browser-Einstellungen verwenden) festgelegt ist.
- Um zur Anzeige einer bestimmten Sprache den Onboard Administrator-Bildschirm „User Preferences“ (Benutzereinstellungen) (Benutzereinstellungen auf Seite 56) zu verwenden, wählen Sie die Sprache aus der Liste „User Preferences“ (Benutzereinstellungen) unter den verfügbaren Sprachen aus und klicken Sie auf **Apply** (Übernehmen). Diese Einstellung überschreibt die aktuelle Spracheinstellung des Browsers und wird bei nachfolgenden GUI-Sitzungen, die eine Verbindung mit dem gleichen Onboard Administrator aufbauen, beibehalten. Die Einstellung gilt jedoch nicht für GUI-Sitzungen mit anderen Onboard Administrator-Modulen. (Die Einstellung basiert auf einem Cookie, das nur für die aktuelle Onboard Administrator-IP-Adresse gültig ist. Wenn sich die IP-Adresse ändert, muss die Einstellung erneut über die neue Adresse übernommen werden.) Um sicherzustellen, dass alle Seiten der Onboard Administrator-GUI die ausgewählte Sprache erben, klicken Sie unten im Bildschirm „User Preferences“ (Benutzereinstellungen) auf **Aktualisieren**.

Jede dieser Einstellungen ist browserspezifisch. Eine Spracheinstellung für Internet Explorer wirkt sich beispielsweise nicht auf die Einstellung für Firefox aus. Es ist nicht zwingend erforderlich, bei allen Browsern die gleiche Methode zu verwenden. Damit die Einstellung nach dem Konfigurieren der bevorzugten Sprache wirksam wird, muss die Webseite möglicherweise aktualisiert oder neu geladen werden.

HINWEIS: Sollte die Anzeigesprache nicht korrekt geladen werden, dann löschen Sie das Browsercache und aktualisieren Sie die Anwendung durch Aktualisieren oder Neuladen des Browsers.

Wenn Sie bei einem primären Gehäuse mit verbundenen Gehäusen angemeldet sind, müssen Sie sicherstellen, dass alle verbundenen Gehäuse über eine mit dem installierten Sprachpaket kompatible Sprachpaketversion verfügen.

Systemprotokoll

Hier werden protokollierte Informationen zu Ereignissen innerhalb Onboard Administrator angezeigt.

Ereignisse werden chronologisch protokolliert, wobei das zuletzt protokollierte Ereignis ganz oben in der Liste angezeigt wird. Innerhalb des Systemprotokolls kann mithilfe der Bildlaufleiste auf der rechten Seite des Protokollbildschirms ein Bildlauf durchgeführt werden (wenn das Protokoll über das Anzeigefeld hinausgeht).

Das Protokoll besitzt eine maximale Kapazität von ca. 18 KB. Wenn das Protokoll diese Kapazität erreicht, löscht es automatisch zuerst das älteste protokollierte Ereignis („first in, first out“).

Um die Liste aller protokollierten Ereignisse im Systemprotokoll zu löschen, klicken Sie auf die Schaltfläche **Clear Log** (Protokoll löschen) rechts unten unterhalb der Anzeige des Systemprotokolls.

Erweitertes Systemprotokoll

Onboard Administrator speichert automatisch 300 KB der neuesten Systemprotokollchronik. Dieses erweiterte Systemprotokoll wird bei einem Neustart und beim Ausschalten beibehalten, sofern diese Aktionen ordnungsgemäß ausgeführt werden. Unter optimalen Bedingungen speichert Onboard

Administrator automatisch bis zu 400 KB der neuesten Systemprotokollchronik. Sollte die Stromversorgung des Onboard Administrator unerwartet ausfallen oder sollte Onboard Administrator aus dem Gehäuse entfernt werden, ohne ordnungsgemäß heruntergefahren zu werden, gehen die neuesten (ungespeicherten) Teile des erweiterten Systemprotokolls möglicherweise verloren.

Mit dem CLI-Befehl `SHOW SYSLOG HISTORY` können Sie das erweiterte Systemprotokoll anzeigen.

Remote-Systemprotokollierung

Die Remote-Systemprotokollierung ermöglicht Ihnen, Onboard Administrator-Syslog-Meldungen zur permanenten Speicherung an einen Remote-Server im Netzwerk zu senden. Sie können diese Funktion auf der Registerkarte „Log Options“ (Protokolloptionen) (Registerkarte „Log Options“ (Protokolloptionen) auf Seite 227) einrichten.

Registerkarte „Log Options“ (Protokolloptionen)

Über diesen Bildschirm können Sie Systemprotokollmeldungen zur permanenten Speicherung an einen Remote-Server im Netzwerk senden. Das lokale Systemprotokoll ist standardmäßig aktiviert. Sie sind nur als „Administrator“ oder als „Operator“ (Bediener) mit OA-Einschubsberechtigungen zur Verwaltung der Systemprotokolleinstellungen berechtigt.

Die Systemprotokollmeldungen werden von Onboard Administrator über das UDP-Protokoll auf einem Port gesendet, der vom Benutzer angegeben werden kann. Der StandardRemote-Port für das Systemprotokoll ist 514.

Die Remote-Systemprotokollierungsfunktion von Onboard Administrator folgt den Richtlinien in RFC3164 (http://www.ietf.org/rfc/rfc3164.txt).

Auf den meisten Linux-Systemen kann die Remote-Systemprotokollierung aktiviert werden, indem der Befehl „syslogd“ mit der Option „-r“ gestartet wird. Der Remote-Port für das Systemprotokoll muss außerdem in der Firewall geöffnet sein. Weitere Informationen finden Sie in der Dokumentation der betreffenden Distribution. Windows® besitzt keine native Unterstützung für die Remote-Systemprotokollierung. Jede Anwendung, die für den UDP-Port 514 oder den angegebenen Systemprotokollport konfiguriert ist, kann Remote-Systemprotokollmeldungen vom Onboard Administrator empfangen.

Aktivieren Sie zum Senden von Systemprotokollmeldungen an einen Remote-Host das Kontrollkästchen **Enable remote system logging** (Remote-Systemprotokollierung aktivieren). Geben Sie den Server und den Port an.

Nachdem die Remote-Systemprotokollierungsfunktion von Onboard Administrator konfiguriert wurde, kann sie mit der Schaltfläche „GUI Test“ (GUI-Test) oder dem CLI-Befehl `TEST SYSLOG` getestet werden.

Feld	Möglicher Wert	Beschreibung
Syslog Server Address (Systemprotokoll-Serveradresse)	• IPv4-Adresse — ###.###.###.###, wobei ### im Bereich von 0 bis 255 liegt. • IPv6-Adresse — ####:####:####:###:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. • DNS-Name — 1 bis 64 Zeichen einschließlich aller	Eine IPv4-Adresse, IPv6-Adresse oder der DNS-Name des Remote-Hosts*

Feld	Möglicher Wert	Beschreibung
	alphanumerischen Zeichen und des Bindestrichs (-).	
Port	Eine ganze Zahl zwischen 1 und 65535.	Der IP-Port des Remote-Hosts.

* Verwenden Sie eine IPv6-Adresse als Remote-Systemprotokollserver.

Klicken Sie auf **Test Remote Log** (Remote-Protokoll testen), um eine Testnachricht an die Remote-Host-Adresse und das lokale Systemprotokoll zu senden. Zur Verwendung dieser Funktion müssen Sie die Remote-Systemprotokollierung aktivieren.

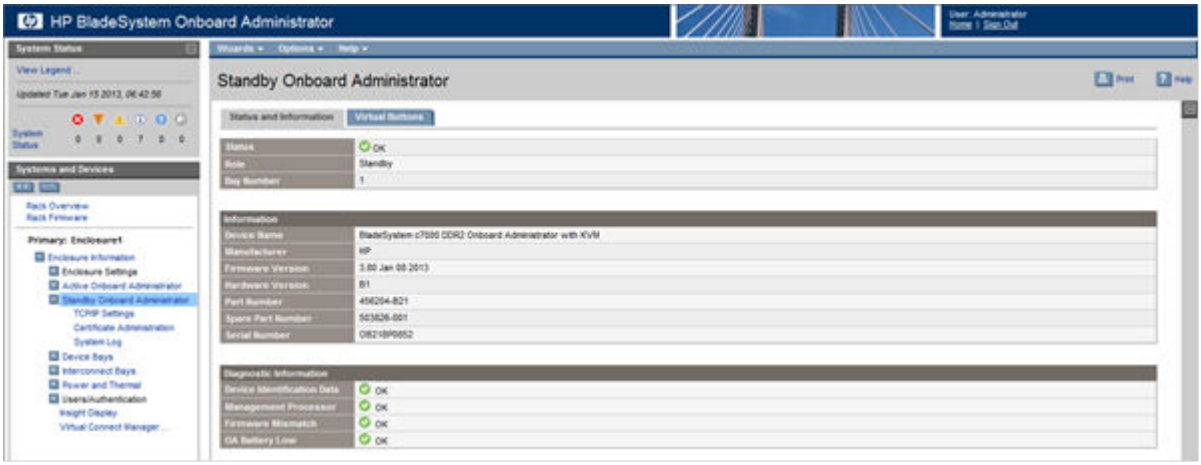
Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Onboard Administrator Standby-Modul

Bildschirm „Standby Onboard Administrator“

Wenn Sie einen zweiten Onboard Administrator im Gehäuse installieren, wird dieser zum Onboard Administrator-Standby-Modul. Das Onboard Administrator-Standby-Modul wird in der Regel im verfügbaren Onboard Administrator-Fach im hinteren Bereich des Gehäuses eingebaut. Über den Bildschirm „Active to Standby“ (Aktiv in Standby) können Sie einen Wechsel innerhalb der Onboard Administrator-Benutzeroberfläche erzwingen, um das aktive Onboard Administrator-Modul zum Onboard Administrator-Standby-Modul zu machen.

Voraussetzung für den Wechsel zwischen aktivem und Standby-Modul ist, dass auf beiden Onboard Administrator-Modulen die gleiche Firmware-Version installiert ist. Wenn die Firmware-Versionen nicht identisch sind, wird dieser Fehler vom Insight Display und im Haupt-Statusbildschirm von Onboard Administrator erkannt, und Benutzer werden per SNMP benachrichtigt (falls aktiviert).



Bei Verwendung von zwei Onboard Administrator-Modulen verfügt jeder Onboard Administrator über eine eindeutige IP-Adresse. Suchen Sie in Insight Display nach den IP-Adressen für das aktive Onboard Administrator-Modul und das Onboard Administrator-Standby-Modul, und notieren Sie sie. Wenn Sie das Gehäuse von hinten betrachten, ist der Schacht auf der linken Seite Schacht 1 und der Schacht auf der rechten Seite Schacht 2. Wenn der aktive Onboard Administrator in den Standby Onboard Administrator wechselt, bleiben der DNS-Hostname und die IP-Adressen gleich. Wenn Sie eine Verbindung zum neuen aktiven HP Onboard Administrator-Modul herstellen möchten, müssen

Sie Ihren Browser vollständig schließen, und eine Verbindung mit dem Hostnamen oder der IP-Adresse des ehemaligen Onboard Administrator-Standby-Moduls herstellen.

Registerkarten „Status“, „Information“ und „Virtual Buttons“ (Virtuelle Tasten)

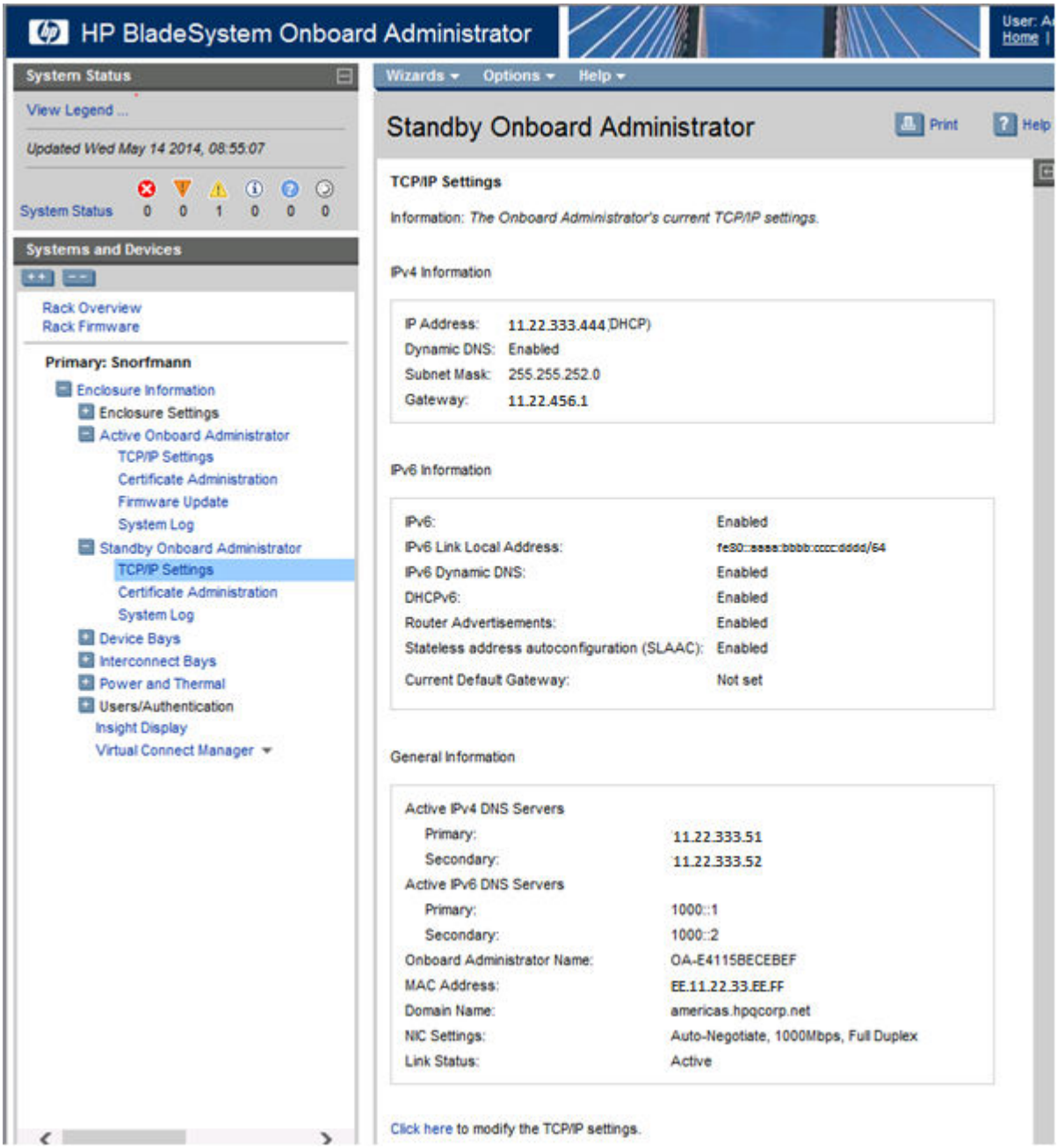
Die Informationen auf den Registerkarten „Status“, „Information“ und „Virtual Buttons“ (Virtuelle Tasten) sind mit denen für ein aktives Onboard Administrator-Modul identisch. Informationen zu diesen Registerkarten finden Sie unter „Aktiver Onboard Administrator“ (siehe Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator) auf Seite 208).

Registerkarte „Virtual Buttons“ des Onboard Administrator-Standby-Moduls

Klicken Sie auf **Reset** (Zurücksetzen), um das Onboard Administrator-Modul zurückzusetzen. Auf einem Bestätigungsbildschirm wird angefragt, ob der Vorgang wirklich durchgeführt werden soll, und darauf hingewiesen, dass der Benutzer abgemeldet und vom Onboard Administrator-Modul getrennt wird. Klicken Sie auf **OK**, um fortzufahren, oder auf **Cancel** (Abbrechen), um den Bildschirm ohne Änderung zu schließen.

Klicken Sie auf **Toggle On/Off** (Ein-/Ausschalten), um den Status der UID-LED des Onboard Administrator-Moduls zu ändern. Dadurch wird ein bestimmter Onboard Administrator identifiziert, wenn mehr als einer vorhanden ist.

Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA



Dieser über die GUI des aktiven Onboard Administrator aufgerufene Bildschirm zeigt die aktuellen Gehäuse-TCP/IP-Einstellungen für den Standby-Onboard Administrator an.

Informationen zu den auf diesem Bildschirm angezeigten TCP/IP-Einstellungen finden unter „Bildschirm ‚TCP/IP Settings' (TCP/IP-Einstellungen) des aktiven Onboard Administrator" (Bildschirm „TCP/IP Settings" (TCP/IP-Einstellungen) des aktiven Onboard Administrator auf Seite 212).

Um die TCP/IP-Einstellungen zu ändern, wählen Sie **Click here** (Hier klicken). Informationen zu den TCP/IP-Einstellungen, die geändert werden können, finden Sie unter „‚Enclosure TCP/IP Settings' (Gehäuse-TCP/IP-Einstellungen)" (Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) auf Seite 126).

Über die Standby-Onboard Administrator-GUI angezeigte Standby-TCP/IP-Einstellungen

Der über die Standby-Onboard Administrator-GUI angezeigte Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) besitzt vier Registerkarten:

- IPv4 Settings (IPv4-Einstellungen)
- IPv6 Settings (IPv6-Einstellungen)
- NIC Options (NIC-Optionen)
- Advanced Settings (Erweiterte Einstellungen)

Diese Registerkarten zeigen die Einstellungen an, die auf dem vorherigen Beispielbildschirm zu sehen sind, und auf Ihnen können zudem viele der Einstellungen direkt geändert werden.

Auf den Registerkarten „IPv4 Settings“ (IPv4-Einstellungen) und „IPv6 Settings“ (IPv6-Einstellungen) können die meisten Einstellungen geändert werden, die auf den entsprechenden Registerkarten auf dem GUI-Bildschirm „Enclosure TCP/IP Settings“ (Gehäuse-TCP/IP-Einstellungen) des aktiven Onboard Administrator geändert werden können. Die Ausnahmen werden in den folgenden Abschnitten beschrieben. Auf den Registerkarten „NIC Options“ (NIC-Optionen) und „Advanced Settings“ (Erweiterte Einstellungen) können die gleichen Einstellungen geändert werden, die auf den entsprechenden Registerkarten auf dem GUI-Bildschirm „Enclosure TCP/IP Settings“ (Gehäuse-TCP/IP-Einstellungen) des aktiven Onboard Administrator geändert werden können.

Ausnahmen für „IPv4 Settings“ (IPv4-Einstellungen)

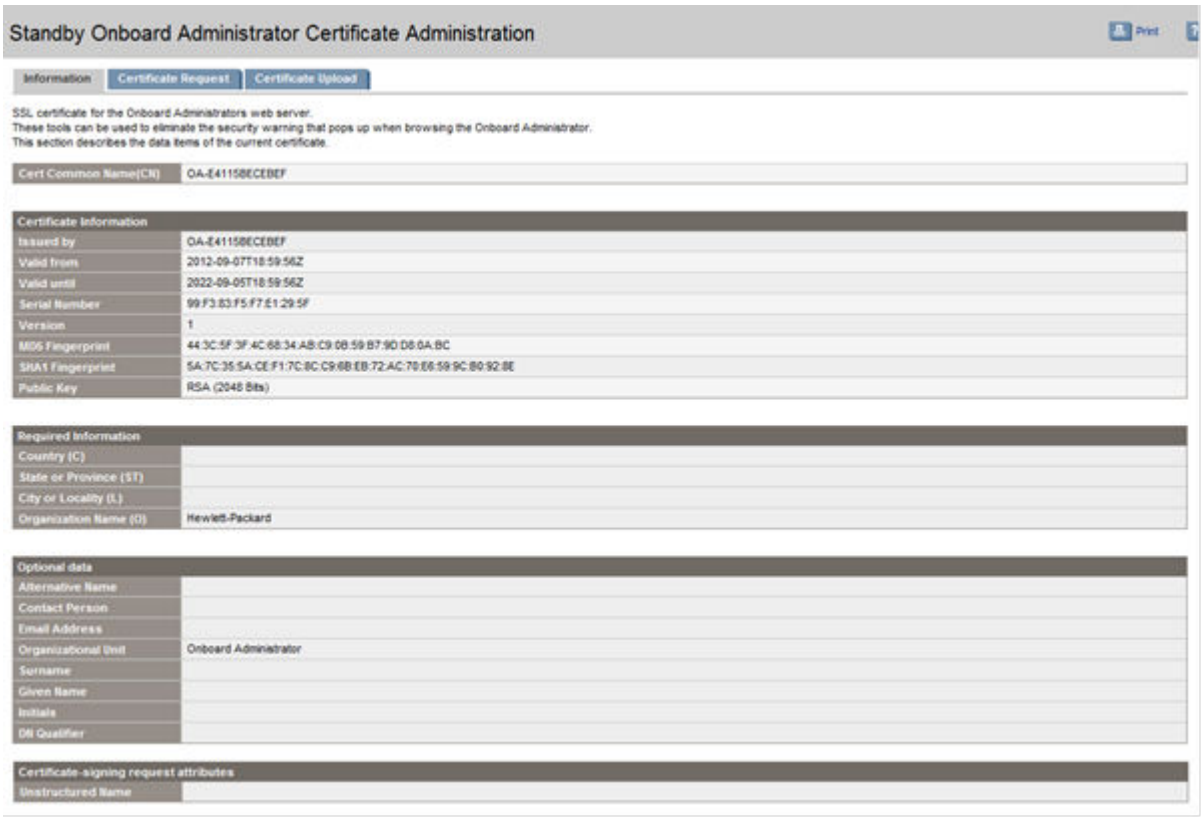
Die Einstellung **Enclosure IP Mode** (Gehäuse-IP-Modus) kann nicht über die Standby-Onboard-Administrator-GUI geändert werden. Sie kann über die Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) auf dem GUI-Bildschirm „Enclosure TCP/IP Settings“ (Gehäuse-TCP/IP-Einstellungen) des aktiven Onboard Administrator geändert werden (Registerkarte „IPv4-Einstellungen“ auf Seite 126).

Ausnahmen für „IPv6 Settings“ (IPv6-Einstellungen)

Die folgenden Einstellungen können nicht über die Standby-Onboard-Administrator-GUI geändert werden. Sie können über die Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf dem GUI-Bildschirm „Enclosure TCP/IP Settings“ (Gehäuse-TCP/IP-Einstellungen) des aktiven Onboard Administrator geändert werden (Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) auf Seite 129).

- **Enclosure IP Mode (Gehäuse-IP-Modus)**
- **Enable IPv6 (IPv6 aktivieren)**
- **Enable Router Advertisements (Routerankündigungen aktivieren)**
- **Enable SLAAC (SLAAC aktivieren)**
- **Enable DHCPv6 (DHCPv6 aktivieren)**

Registerkarte „Information“ (Informationen) auf dem Bildschirm „Standby Onboard Administrator Certificate Administration“ (Zertifikatverwaltung des Onboard Administrator-Standby-Moduls)



Registerkarte „Information“

Dieser Bildschirm zeigt detaillierte Informationen zu dem derzeit von Onboard Administrator verwendeten SSL-Zertifikat an. Ein SSL-Zertifikat dient zur Bescheinigung der Identität von Onboard Administrator und wird von dem zugrunde liegenden HTTP-Server zum Aufbau einer sicheren (verschlüsselten) Kommunikationsverbindung mit dem Client-Web-Browser vorgeschrieben.

Beim ersten Starten erstellt Onboard Administrator ein 10 Jahre lang gültiges, selbstsigniertes SSL-Standardzertifikat, das auf den Namen des Onboard Administrator-Moduls ausgestellt ist. Da dieses Standardzertifikat selbstsigniert ist, wird das Feld „Issued by“ (Ausgestellt von) auf den gleichen Namen eingestellt.

Statusinformationen

Zeile	Beschreibung
Cert Common Name (Allgemeine Name des Zertifikats)	Der allgemeine Name des Zertifikats.

Certificate Information (Informationen zum Zertifikat)

Zeile	Beschreibung
Issued by (Ausgestellt von)	Die Zertifizierungsstelle, die das Zertifikat ausgestellt hat.

Zeile	Beschreibung
Valid from (Gültig ab)	Das Datum, ab dem das Zertifikat gültig ist.
Valid until (Gültig bis)	Das Datum, an dem das Zertifikat abläuft.
Serial Number (Seriennummer)	Die dem Zertifikat von der Zertifizierungsstelle zugewiesene Seriennummer.
Version	Die Versionsnummer des aktuellen Zertifikats.
MD5 Fingerprint (MD5-Fingerabdruck)	Dieses im Zertifikat eingebettete Feld dient der Echtheitsprüfung.
SHA1 Fingerprint (SHA1-Fingerabdruck)	Dieses im Zertifikat eingebettete Feld dient der Echtheitsprüfung.
Public Key (Öffentlicher Schlüssel)	Der Name des öffentlichen Schlüssels.

Benötigte Informationen

Zeile	Beschreibung
Country (C) (Land):	Ein zweistelliger Landescode, durch den das Land identifiziert wird, in dem sich Onboard Administrator befindet.
State or Province (ST) (Bundesstaat oder Provinz):	Der Bundesstaat oder die Provinz, in der sich Onboard Administrator befindet.
City or Locality (L) (Stadt oder Ort):	Die Stadt oder der Ort, in der bzw. an dem sich Onboard Administrator befindet.
Organization Name (O) (Name der Organisation):	Die Firma, in deren Besitz sich dieser Onboard Administrator befindet.

Optional data (Optionale Daten)

Zeile	Beschreibung
Alternative Name (Alternativer Name)	Ein alternativer Name für den Onboard Administrator.
Contact Person (Kontaktperson)	Die für Onboard Administrator verantwortliche Person.
Email Address (E-Mail-Adresse)	Die E-Mail-Adresse der für Onboard Administrator verantwortlichen Person.
Organizational Unit (Organisationseinheit)	Die Einheit innerhalb der Firma oder Organisation, in deren Besitz sich Onboard Administrator befindet.
Surname (Vorname)	Der Vorname der für Onboard Administrator verantwortlichen Person.
Given Name (Nachname)	Der Nachname der für Onboard Administrator verantwortlichen Person.
Initials (Initialen)	Die Initialen der für Onboard Administrator verantwortlichen Person.
DN Qualifier (DN-Kennzeichner)	Der eindeutige Namenskennzeichner von Onboard Administrator.

Certificate-signing request attributes (Zertifikatssignierungs-Anforderungsattribute)

Zeile	Beschreibung
Unstructured Name (Unstrukturierter Name)	Dies sind zusätzliche Informationen.

Registerkarte „Certificate Request“ (Zertifikat-Anforderung) des Standby-Moduls

Auf der Registerkarte „Certificate Request“ (Zertifikat-Anforderung) des Standby-Moduls können Sie die Informationen eingeben, die zum Erstellen eines selbstsignierten Zertifikats oder einer genormten Zertifikatssignierungsanforderung an eine Zertifizierungsstelle erforderlich sind.

Benötigte Informationen

Feld	Mögliche Werte	Beschreibung
Country (C) (Land)	Der Ländercode muss zweistellig sein. Zulässige Zeichen sind alle alphanumerischen Zeichen, ein Leerzeichen und die folgenden Satzzeichen: ' ( ) + , - . / : = ?	Ein zweistelliger Landescode, durch den das Land identifiziert wird, in dem sich Onboard Administrator befindet.
State or Province (ST) (Bundesstaat oder Provinz)	Muss 1 bis 30 Zeichen lang sein.	Der Bundesstaat oder die Provinz, in der sich Onboard Administrator befindet.
City or Locality (L) (Stadt oder Ort)	Muss 1 bis 50 Zeichen lang sein.	Die Stadt oder der Ort, in der bzw. an dem sich Onboard Administrator befindet.
Organization Name (O) (Name der Organisation)	Muss 1 bis 60 Zeichen lang sein.	Die Organisation, in deren Besitz sich dieser Onboard Administrator befindet. Wenn anhand dieser Informationen eine Zertifikatssignierungsanforderung erstellt wird, kann die ausstellende Zertifizierungsstelle prüfen, ob die das Zertifikat anfordernde Organisation gesetzlich dazu berechtigt ist, sich als Besitzer des betreffenden Firmennamens oder der betreffenden Organisation auszugeben.
Common Name (CN) (Allgemeiner Name)	Muss 1 bis 60 Zeichen lang sein. Damit keine Sicherheitswarnungen ausgegeben werden, muss der Wert dieses Feldes genau dem Hostnamen entsprechen, der dem Web-Browser bekannt ist. Der Browser vergleicht den Hostnamen in der aufgelösten Webadresse mit dem im Zertifikat angegebenen Namen. Lautet die Webadresse im Adressfeld beispielsweise https://oa-001635.xyz.com, muss der Wert oa-001635.xyz.com lauten.	Der im Web-Adressfeld des Browsers angezeigte Onboard Administrator-Name. Dieses Zertifikatattribut wird in der Regel als der geläufige Name bezeichnet.

Um eine Anforderung für ein Zertifikat des aktiven Onboard Administrator einzuschließen, wählen Sie **Active OA Host Name** (Hostname des aktiven OA). Geben Sie die Informationen in das Feld **Active Common Name (CN)** (Allgemeiner Name des aktiven Moduls (CN)) ein. Der Eintrag muss 1 bis 60 Zeichen lang sein.

Optional Information (Optionale Informationen)

Feld	Mögliche Werte	Beschreibung
Alternative Name (Alternativer Name)	Muss 0 bis 511 Zeichen lang sein.	Ein alternativer Name für den Onboard Administrator. Der Name wird zum Erstellen des Erweiterungsattributs „X509v3 Subject Alternative Name“ verwendet. Das Feld muss entweder leer sein oder eine Liste von durch Kommas getrennter Schlüsselwort:Wert-Paare enthalten. Zu den gültigen Schlüsselwort:Wert-Einträgen gehören IP:<IP-Adresse> und DNS:<Domänenname>.
Contact Person (Kontaktperson)	Muss 0 bis 60 Zeichen lang sein.	Die für Onboard Administrator verantwortliche Person.
Email Address (E-Mail-Adresse)	Muss 0 bis 60 Zeichen lang sein.	Die E-Mail-Adresse der für Onboard Administrator verantwortlichen Kontaktperson.
Organizational Unit (Organisationseinheit)	Muss 0 bis 60 Zeichen lang sein.	Die Einheit innerhalb der Firma oder Organisation, in deren Besitz sich Onboard Administrator befindet.
Surname (Vorname)	Muss 0 bis 60 Zeichen lang sein.	Der Vorname der für Onboard Administrator verantwortlichen Person.
Given Name (Nachname)	Muss 0 bis 60 Zeichen lang sein.	Der Nachname der für Onboard Administrator verantwortlichen Person.
Initials (Initialen)	Muss 0 bis 20 Zeichen lang sein.	Die Initialen der für Onboard Administrator verantwortlichen Person.
DN Qualifier (DN-Kennzeichner)	Muss 0 bis 60 Zeichen lang sein. Zulässige Zeichen sind alle alphanumerischen Zeichen, das Leerzeichen sowie die folgenden Satzzeichen: ' ( ) + , - . / : = ?	Der eindeutige Namenskennzeichner von Onboard Administrator.

Certificate-signing request attributes (Zertifikatssignierungs-Anforderungsattribute)

Feld	Mögliche Werte	Beschreibung
Challenge Password (Kennwort)	Muss 0 bis 30 Zeichen lang sein.	Das Kennwort der Zertifikatssignierungsanforderung.
Confirm Password (Kennwortbestätigung)	Muss 0 bis 30 Zeichen lang sein.	Dient zur Bestätigung des Kennworts.
Unstructured Name (Unstrukturierter Name)	Muss 0 bis 60 Zeichen lang sein.	Dieses Feld ist für Zusatzinformationen bestimmt, beispielsweise für einen Onboard Administrator zugewiesenen unstrukturierten Namen.

Klicken Sie auf **Apply** (Übernehmen). Es wird ein selbstsigniertes Zertifikat bzw. eine genormte Zertifikatssignieranforderung erstellt.

Standardized certificate-signing request (Genormte Zertifikatssignieranforderung)

Dieser Bildschirm zeigt eine von Onboard Administrator erstellte genormte Zertifikatssignieranforderung an. Der Inhalt der Anforderung im Textfeld kann zwecks Signierung an eine Zertifizierungsstelle Ihrer Wahl gesendet werden. Das von der Zertifizierungsstelle zurückgesandte signierte Zertifikat kann auf der Registerkarte „Certificate Upload“ (Zertifikat-Upload) hochgeladen werden.

War für Onboard Administrator eine statische IP-Adresse konfiguriert, als diese Zertifikatanforderung erstellt wurde, wird die Anforderung an die statische IP-Adresse ausgegeben. Andernfalls wird sie an den dynamischen DNS-Namen von Onboard Administrator ausgegeben. Das Zertifikat fordert standardmäßig eine Gültigkeitsdauer von 10 Jahren an (dieser Wert kann derzeit nicht konfiguriert werden).

Beim Senden der Anforderung an die Zertifizierungsstelle müssen Sie auf Folgendes achten:

1. Verwenden Sie die Onboard Administrator-Internet-Adresse (URL) für den Server.
2. Fordern Sie die Erzeugung des Zertifikats im RAW-Format an.
3. Schließen Sie die Zertifikatzeilen „Begin“ und „End“ ein.

Registerkarte „Certificate Upload“ (Zertifikat-Upload) des Standby-Moduls

Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Das hochzuladende Zertifikat muss sich auf eine Zertifikatsanforderung für den betreffenden Onboard Administrator zurückführen lassen, die an eine Zertifizierungsstelle gesendet und von ihr signiert wurde. Andernfalls stimmt das Zertifikat nicht mit den privaten Schlüsseln überein, die zur Erstellung der Zertifikatsanforderung verwendet wurden, und wird zurückgewiesen. Wurde die Onboard Administrator-Domäne zerstört oder neu importiert, müssen die Schritte zur Erstellung einer Zertifikatanforderung ebenfalls wiederholt werden. Es wird von einer Zertifizierungsstelle neu zugewiesen, da die privaten Schlüssel zusammen mit der Onboard Administrator-Domäne zerstört und neu erstellt werden.

Nachdem das neue Zertifikat von Onboard Administrator akzeptiert und erfolgreich installiert wurde, werden Sie automatisch abgemeldet. Der HTTP-Server muss neu gestartet werden, damit das neue Zertifikat wirksam wird.

Weitere Informationen zur Subkategorie „System Log“ (Systemprotokoll) finden Sie unter „System Log (Systemprotokoll)“ (Systemprotokoll auf Seite 226).

Systemprotokoll für Standby-Onboard Administrator

Das Systemprotokoll zeigt protokollierte Informationen zu Ereignissen innerhalb Onboard Administrator an.

Ereignisse werden vom Anfang der Liste bis zum Ende chronologisch protokolliert, wobei das zuletzt protokollierte Ereignis am Ende der Liste steht. Listen, die länger als das Anzeigefeld sind, können mit Hilfe der Bildlaufleiste auf der rechten Seite des Protokollbildschirms durchlaufen werden.

Wenn das Protokoll die maximale Kapazität erreicht, löscht es automatisch zuerst das älteste protokollierte Ereignis („first in, first out“).

Wenn Sie die Liste aller protokollierten Ereignisse löschen möchten, klicken Sie auf **Clear Log** (Protokoll löschen) unterhalb der Systemprotokollanzeige.

Standby to Active (Standby in Aktiv)

Um den Standby-Onboard Administrator in den aktiven Onboard Administrator zu verwandeln, klicken Sie auf **Transition Standby to Active** (Von Standby-Modul in aktives Modul wechseln). In einem Bestätigungsbildschirm werden Sie aufgefordert zu bestätigen, dass der Vorgang durchgeführt werden soll. Um fortzufahren, klicken Sie auf **OK**. Um den Vorgang zu beenden, ohne eine Änderung vorzunehmen, klicken Sie auf **Cancel** (Abbrechen).

Diese Funktionalität ist nur verfügbar, wenn Sie bei dem Standby-Onboard Administrator-Modul angemeldet sind.

Sie können den Wechsel vpm Standby-Onboard Administrator in den aktiven Onboard Administrator auch mit dem CLI-Befehl FORCE TAKEOVER erzwingen.

Die Dauer des Wechsels vom Standby-Modul in das aktive Modul bzw. vom aktiven Modul in das Standby-Modul ist je nach Konfiguration, Gehäuse-Bestückung und verschiedenen anderen Faktoren verschieden. Wenn das zuvor aktive Onboard Administrator-Modul während dieses Wechsels vorzeitig entfernt wird, dauert der Wechsel von „Standby“ zu „Aktiv“ länger.

Geräteeinschübe

Geräteeinschübe

Zusammenfassung des Geräteeinschubs

Im Menü „Systems and Devices“ (Systeme und Komponenten) werden in der Kategorie „Device Bays“ (Geräteeinschübe) alle Blades innerhalb des Gehäuses aufgelistet. Durch Auswahl der Menüoption „Device Bays“ (Geräteeinschübe) wird die Komponentenliste mit einer Tabelle angezeigt, aus der der Status der einzelnen Blades innerhalb des Gehäuses hervorgeht.

Das Kontrollkästchen in der obersten Zeile in der ersten Spalte schaltet den Status aller Kontrollkästchen für alle Blades innerhalb des Gehäuses um. Es kann zum Aus- und erneutem Einschalten aller Server Blades innerhalb des Gehäuses verwendet werden. Optional können die einzelnen Kontrollkästchen zur Auswahl spezifischer Blades verwendet werden. Nachdem die Blades ausgewählt wurden, wählen Sie aus den Menüs die Optionen „Virtual Power“ (Virtueller Netzschalter), „UID State“ (UID-Zustand), „One Time Boot“ (Einmaliges Booten), „DVD“ oder „Enclosure Management“ aus, um die entsprechende Aktion durchzuführen. Virtuelle Befehle gelten nicht für Speicher-Blades.

Komponentenliste

Spalte	Beschreibung
Kontrollkästchen	Wählen Sie durch Aktivieren des Kontrollkästchens für die gewünschten Blades die Einschübe aus, auf die die Aktionen „Virtual Power“ (Virtueller Netzschalter), „UID State“ (UID-Status), „One Time Boot“ (Einmaliges Booten), „DVD“ oder „Firmware Management“ (Firmware-Management) angewandt werden sollen.
Bay (Einschub)	Der Geräteeinschub innerhalb des Gehäuses.
Status (Zustand)	Der allgemeine Status der Komponente. Die möglichen Werte sind „OK“ und „Enclosure Firmware Management“.
UID	Der Status der UID für die Komponente. Mögliche Werte sind „On“ (Ein) (blau), „Off“ (Aus) (grau) oder Blinken. Wenn die UID-LED blinkt, wird gerade ein wichtiger Vorgang auf der Komponente ausgeführt, der nicht unterbrochen werden darf.

Spalte	Beschreibung
Power State (Stromversorgungsstatus)	Der Stromversorgungsstatus der Komponente. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
iLO IP Address (iLO IP-Adresse)	Die IP-Adresse der iLO innerhalb der Server Blade. Gilt nicht für Speicher-Blades. Um eine Verbindung zum iLO herzustellen, klicken Sie auf den IP-Adressen-Link. Um festzustellen, ob alle iLO-IP-Adressen-Links verfügbar sind, klicken Sie auf den Abwärtspfeil rechts neben der iLO-IP-Adresse. In einem Popup-Fenster erscheinen die Internet-Adressen-Links, über die Sie eine Verbindung zum iLO herstellen können. Wenn FQDN-Link-Unterstützung aktiviert ist und bestimmten DNS-Konfiguration-Anforderungen entsprochen wird, wird als Standardoption eine FQDN-basierte Internetadresse vorgegeben. Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).
iLO Name	Der DNS-Name der iLO innerhalb der Server Blade. Gilt nicht für Speicher-Blades.
iLO DVD Status (ilO DVD-Status)	Der Status der DVD-Verbindung zum Server Blade. Mögliche Werte sind „Connected“ (Verbunden), „Disconnected“ (Getrennt) oder „Unknown“ (Unbekannt). Lautet der Status „Inkompatible Firmware“, bedeutet dies, dass die DVD-Funktion nicht mit der auf der Komponente installierten iLO Firmware unterstützt wird. Der Status „Unknown“ (Unbekannt) weist auf ein iLO-Verbindungsproblem hin.

Die Informationen auf dieser Seite entsprechen dem letzten Download. Um die aktualisierten Informationen anzuzeigen, klicken Sie auf **Refresh** (Aktualisieren).

UID State (UID-Status)

Das Dropdown-Menü „UID State“ (UID-Status) wird verwendet, um die UID-LED an den Blades einzustellen. Durch Einschalten der UID-LED ist ein bestimmter Blade innerhalb eines Gehäuses leichter auffindbar. Die UID-LEDs lassen sich abhängig von den Kontrollkästchen einzeln oder gruppenweise ein- und ausschalten.

Virtual Power (Virtueller Netzschalter)

Befehle für den virtuellen Netzschalter gelten nicht für Partner-Blades.

Schaltfläche	Beschreibung
Momentary Press (Kurzes Drücken)	Diese Schaltfläche ahmt ein kurzes physisches Drücken des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade ordnungsgemäß ein- oder ausgeschaltet.
Press and Hold (Rastendes Drücken)	Diese Schaltfläche ahmt ein physisches Drücken und Halten des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade zum Ausschalten gezwungen, ohne zuvor zuerst das Betriebssystem herunterzufahren. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.
Cold Boot (Kaltstart)	Bei Anklicken dieser Schaltfläche wird die Stromversorgung des Systems sofort unterbrochen. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.
Reset (Zurücksetzen)	Bei Anklicken dieser Schaltfläche wird das System zurückgesetzt. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.

One Time Boot (Einmaliges Booten)

Wenn „Secure Boot“ (Sicherer Systemstart) auf dem Blade im ausgewählten Einschub aktiviert ist, kann dieser Vorgang nicht über die Onboard Administrator-GUI oder -CLI ausgeführt werden. Er kann nur über das im BIOS vom Administrator konfigurierte Gerät ausgeführt werden.

Option	Beschreibung
Diskette Drive (A:) (Diskettenlaufwerk)	Bewirkt einen Neustart des Server Blade über das Diskettenlaufwerk. Vergewissern Sie sich vor Auswahl dieser Option, dass am Server Blade ein Diskettenlaufwerk angeschlossen ist.
CD-ROM	Bewirkt einen Neustart des Server Blade über das CD-ROM-Laufwerk. Vergewissern Sie sich vor Auswahl dieser Option davon, dass am Server Blade ein CD-ROM-Laufwerk angeschlossen ist.
Hard Drive C: (Festplattenlaufwerk C:)	Bewirkt den Neustart des Server Blade von der Festplatte.
RBSU	Bewirkt das Booten des Server Blade über das RBSU (ROM-Based Setup Utility).
PXE NIC	Bewirkt das Booten des Server Blade über PXE NIC.

DVD

Über das Menü „DVD“ können Sie das gemeinsam genutzte DVD-Laufwerk verbinden oder trennen, indem Sie **Connect to Enclosure DVD** (Mit Gehäuse-DVD verbinden) bzw. **Disconnect DVD Hardware** (DVD-Hardware trennen) wählen. Sie können das gemeinsam genutzte DVD-Laufwerk mit mehreren Server Blades verbinden. Nachdem das freigegebene DVD-Laufwerk verbunden wurde, können Sie mit den Optionen im Menü „Virtual Power“ (Virtueller Netzschalter) die ausgewählten Server Blades in der Liste neu starten. Wenn für eine Installation mehrere Mediendatenträger benötigt werden, dann müssen Sie die Verbindung und Trennung möglicherweise für jeden Server durchführen, wenn der neue Mediendatenträger in das DVD-Laufwerk eingelegt wird.

Wenn ein USB-Schlüssel im USB-Port des aktiven Onboard Administrator-Moduls erkannt wird und ISO-Images vorhanden sind, werden diese im DVD-Menü angezeigt. Wählen Sie die Server Blades aus, für die Sie ein ISO-Image bereitstellen möchten, und wählen Sie dann das ISO-Image im Menü aus. Das ISO-Image wird bereitgestellt.

Enclosure Firmware Management

Die manuelle Ermittlung eines oder mehrerer Server kann gestartet werden, um die Erfassung bestehender Firmwareversionen zu vereinfachen.

Nachdem eine manuelle Firmware-Ermittlung gestartet wurde, erscheint der Bildschirm „Manual Discovery Device Bay Selection“ (Geräteeinschubsauswahl für manuelle Ermittlung). Wählen Sie einen oder mehrere Geräteeinschübe aus, auf denen die Ermittlung durchgeführt werden soll. Sie können auch das Kontrollkästchen **Discover All Servers** (Alle Server ermitteln) aktivieren, um alle Server für die Ermittlung auszuwählen. Standardmäßig sind alle Geräteeinschübe und das Kontrollkästchen „Discover All Servers“ (Alle Server ermitteln) ausgewählt.

Wenn „Secure Boot“ (Sicherer Systemstart) auf einem Server Blade konfiguriert ist, kann der zugehörige Einschub nicht ausgewählt werden (es wird das Symbol eines Vorhängeschlosses angezeigt). Der Modus „Secure Boot“ (Sicherer Systemstart) hindert Benutzer daran, eine manuelle Ermittlung über die Onboard Administrator-GUI oder-CLI durchzuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Um den Ermittlungsvorgang auf den ausgewählten Servern zu starten, klicken Sie auf **Start Manual Discovery** (Manuelle Ermittlung starten).

Es kann ein manuelles Update eines oder mehrerer Server zu den angegebenen Firmware-Image-Version initiiert werden. Um eine Firmwareaktualisierung auf einem oder mehreren Servern zu starten, klicken Sie auf **Manual Update** (Manuelle Aktualisierung).

Nachdem eine manuelle Firmwareaktualisierung gestartet wurde, erscheint der Bildschirm „Manual Update Device Bay Selection“ (Geräteeinschubsauswahl für manuelle Aktualisierung). Wählen Sie einen oder mehrere Geräteeinschübe aus, auf denen die Aktualisierung durchgeführt werden soll. Sie können auch das Kontrollkästchen **Update All Servers** (Alle Server aktualisieren) aktivieren, um alle Server für die Aktualisierung auszuwählen. Standardmäßig sind alle Geräteeinschübe und das Kontrollkästchen „Discover All Servers“ (Alle Server ermitteln) ausgewählt.

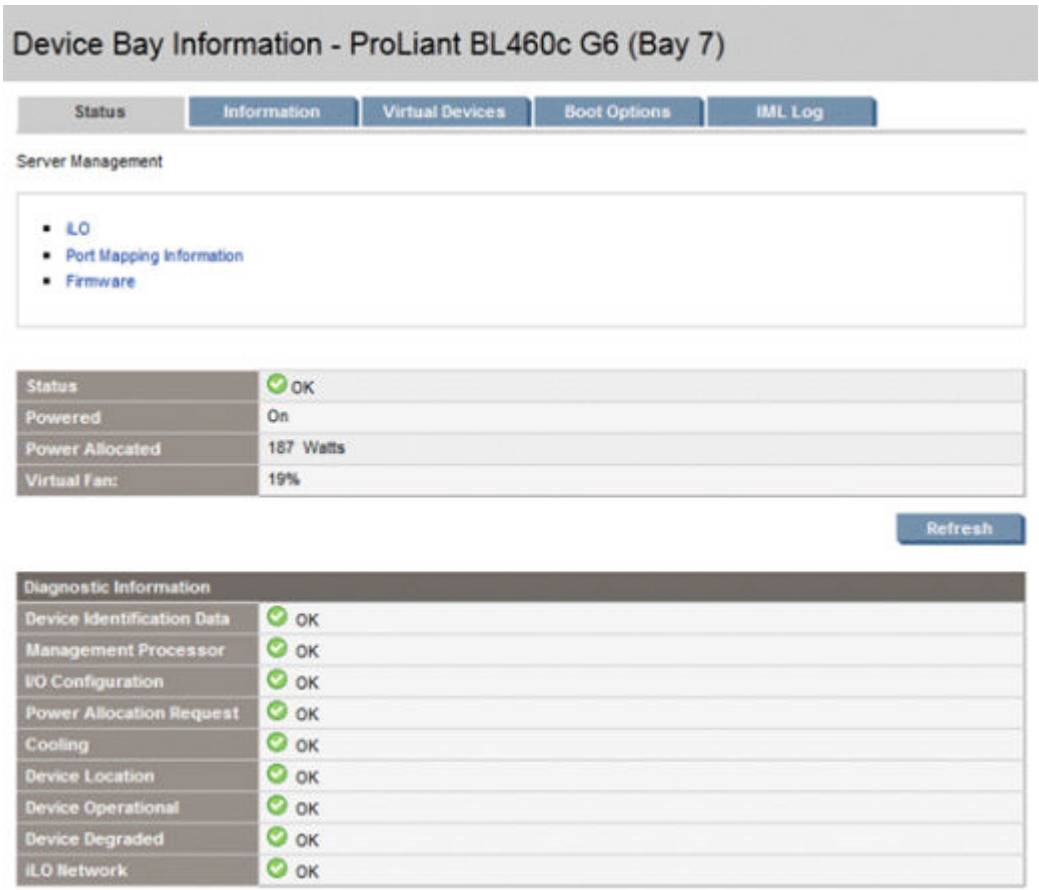
Wenn „Secure Boot“ (Sicherer Systemstart) auf einem Server Blade konfiguriert ist, kann der zugehörige Einschub nicht ausgewählt werden (es wird das Symbol eines Vorhängeschlosses angezeigt). Der Modus „Secure Boot“ (Sicherer Systemstart) hindert Benutzer daran, eine manuelle Aktualisierung über die Onboard Administrator-GUI oder -CLI durchzuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Um den Aktualisierungsvorgang auf den ausgewählten Servern zu starten, klicken Sie auf **Start Manual Update** (Manuelle Aktualisierung starten).

Registerkarte „Device Bay Status“ (Status des Geräteeinschubs)

Durch Auswahl eines bestimmten Blades innerhalb des Gehäuses wird der Bildschirm „Device Bay Information“ (Geräteeinschubs-Informationen) für Einschub *xx*geöffnet, wobei *xx* der ausgewählte Einschub ist. Dieser Bildschirm enthält Registerkarten für „Status“, „Information“ (Informationen), „Virtual Devices“ (Virtuelle Geräte), „Boot Options“ (Boot-Optionen) und „IML Log“ (IML-Protokoll).

Im Bereich „Server Management“ (Serververwaltung) der Seite befinden sich zwei Links zur Erleichterung der Server Blade-Verwaltung im Geräteeinschub.



Zeile	Beschreibung
System Event Health (Systemereignis-Systemzustand)	Der interne Systemereignis-Systemzustand, den die Komponente meldet. Wenn der Status nicht „OK“ ist, untersuchen Sie das Blade-Systemereignisprotokoll für den iLO, um die Ursache für den Zustand festzustellen. Mögliche Werte sind „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Status (Zustand)	Der allgemeine Status des Blade. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt), „Failed“ (Fehler) oder „Other“ (Sonstiges) mit einem informativen Symbol. Das informative Symbol wird zusammen mit der dem Status „Other“ (Sonstiges) angezeigt, solange der Server Blade nicht für Virtual Connect Manager konfiguriert wurde. Weitere Informationen finden Sie in der Tabelle „Diagnostic Information“ (Diagnostische Informationen).
Powered (Netzbetrieb)	Der Stromversorgungsstatus des Blade. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
Power Delay Remaining (Verbleibende Stromzufuhrverzögerung)	Die Anzahl der Sekunden, die verbleiben, bevor die Komponente eingeschaltet wird.
Power Allocated (Zugewiesene Stromversorgung)	Die Menge der dem Blade zugewiesenen Stromversorgung in Watt.
Partner Device (Gepaarte Komponente)	Der Speicher-/Erweiterungs-Blade, mit dem der Server Blade gepaart ist. Diese Informationen werden nicht angezeigt, wenn keine gepaarte Komponente vorhanden ist.
Virtual Fan (Virtueller Lüfter)	Maximale Umdrehungen pro Minute (RPM) des virtuellen Lüfters in Prozent.

Diagnostic information (Diagnoseinformationen)

Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Management Processor (Managementprozessor)	Status von iLO. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Temperature (Temperatur)	Die Temperatur liegt über der Warnschwelle. Mögliche Werte sind „OK“ oder „Temperature Warning“ (Warnung Temperatur).
Overheat Check (Überhitzungskontrolle)	Die Temperatur liegt über der Gefahrenschwelle. Mögliche Werte sind „OK“ und „Critical temperatur threshold reached“ (Kritischer Temperatur-Schwellenwert erreicht).
I/O Configuration (I/O-Konfiguration)	Die Konfiguration des Geräteeinschubs ist inkorrekt. Wenn ein Speicher-Blade mit einem Server Blade voller Bauhöhe gepaart wird und der Server Blade nicht über die richtige Mezzanine Card verfügt, hat dies eine ungültige I/O-Konfiguration zur Folge. Mögliche Werte sind „OK“ oder „I/O Mismatch Detected“ (I/O-Unstimmigkeit ermittelt).
Power Allocation Request (Stromzuweisungsanforderung)	Die verfügbare Stromversorgung ist zum Betreiben dieses Server Blade nicht ausreichend. Mögliche Werte sind „OK“ oder „Insufficient enclosure power“ (Unzureichende Stromversorgung des Gehäuses).
Cooling (Kühlung)	Die Anzahl der Lüfter reicht nicht aus, um diesen Server Blade ordnungsgemäß zu kühlen, oder die Lüfterkonfiguration ist falsch. Mögliche Werte sind „OK“ oder „Insufficient fans for enclosure cooling“ (Unzureichende Lüfter zur Kühlung des Gehäuses).
Device Location (Komponentenposition)	Der Server Blade wurde laut aktueller Lüfterkonfiguration in den falschen Steckplatz im Gehäuse eingebaut. Mögliche Werte sind „OK“ und „Incorrect location for proper device cooling“ (Inkorrekte Position für angemessene Komponentenkühlung).
Device Operational (Komponente betriebsbereit)	Komponente ist ausgefallen. Der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Degraded (Komponente beeinträchtigt)	Komponente ist ausgefallen. Der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
iLO Network (iLO-Netzwerk)	Erkennt ein iLO-Netzwerkkonfigurationsproblem. Mögliche Werte sind „OK“ oder „iLO network configuration problem“ (iLO-Netzwerkkonfigurationsproblem). Überprüfen Sie die Verbindung mit dem iLO-Standard-Gateway. Sollte das Problem fortbestehen, dann versuchen Sie, iLO über die iLO-GUI oder den Onboard Administrator-CLI-Befehl `RESET ILO` zurückzusetzen. Sie können auch mit dem CLI-Befehl `HPONCFG` einen Skriptbefehl zum Zurücksetzen von iLO senden.
Memory Error (Speicherfehler)	Auf dem Server Blade ist ein Speicherfehler aufgetreten. Befolgen Sie zum Beheben des Fehlers die bereitgestellten Anweisungen.
Mezzanine Card	Zeigt einen Fehler an, wenn der Server Blade aufgrund einer fehlenden Mezzanine Card kein Partnerschaft hat. Zeigt „OK“ an, wenn bei der Diagnose einer Einschaltanforderung keine Probleme in der Zusammenarbeit erkannt wurden. Dieser Status wird zurückgesetzt, wenn Onboard Administrator neu gestartet wird.
Duplicate IP Address (Doppelte IP-Adresse)	Eine Kontrolle während der Zuweisung, ob im Netzwerk eine doppelte IP-Adresse vorhanden ist. Mögliche Werte sind „OK“ oder eine informative Meldung, dass im Netzwerk eine doppelte IP-Adresse vorhanden ist.
Enclosure Dynamic Power Capping (Gehäusedynamische Stromobergrenzen)	Eine Warnung, dass die Kommunikation mit dem iLO verloren gegangen ist und keine Stromobergrenze festgelegt werden kann.
Partner Device Link (Verbindung der verbundenen Komponente)	Verbindungsstatus der mit dem Server Blade verbundenen Komponente. Mögliche Werte sind „OK“ oder „Inappropriate device in adjacent bay“ (Inkompatible

Zeile	Beschreibung
	Komponente im benachbarten Einschub). Wenn der Server Blade nicht mit einem Speicher-Blade verbunden ist, werden diese Informationen nicht angezeigt.
Virtual Connect Configured (Virtuelle Verbindung konfiguriert)	Mögliche Werte sind „Configured for Virtual Connect“ (Für virtuelle Verbindung konfiguriert) oder „Not configured for Virtual Connect“ (Nicht für virtuelle Verbindung konfiguriert). Wenn der Server Blade nicht für Virtual Connect konfiguriert ist, erscheint ein informatives Symbol zusammen mit dem Status „Other“ (Sonstiges). Rufen Sie zum Konfigurieren des Server Blade-Profils den Virtual Connect Manager auf.
Low Power Request (Niedrige Stromversorgungsanforderung)	Der Server Blade hat eine ungewöhnlich niedrige Stromanforderung gemeldet. Der Server Blade wurde ausgeschaltet und hat nicht die komplette Leistung freigegeben. Der Server Blade wird weiterhin ordnungsgemäß betrieben werden, aber das Problem sollte durch Kontaktieren eines Servicepartners behoben werden.
Firmware Management (Firmware-Verwaltung)	Der Status der Firmware-Verwaltung auf dem Server.
Power Denial-Discovery (Keine Stromversorgung – Ermittlung)	Die Warnung, dass die Gerätestromversorgung während der Geräteermittlung verzögert wird.
Power Denial-SAS Storage (Keine Stromversorgung – SAS-Speicher)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis der SAS-Speicher bereit ist.
Power Denial-Partnering (Keine Stromversorgung – Partnerschaft)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis das Gerät für Partnerschaft konfiguriert ist.
Power Denial-VC Profile (Keine Stromversorgung – VC-Profil)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis das VC-Profil übernommen wurde.
Power Denial-OA (Keine Stromversorgung – OA-Initialisierung)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis der Onboard Administrator die Initialisierung abgeschlossen hat.
Power Denial-Power Delay (Keine Stromversorgung – Stromversorgungsverzögerung)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis die konfigurierte Stromversorgungsverzögerung für diesen Einschub abgelaufen ist.
Power Denial-Firmware Management (Keine Stromversorgung – Firmware-Management)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis der Firmware-Managementprozess abgeschlossen wurde.
Power Denial-I/O Discovery (Keine Stromversorgung – I/O-Ermittlung)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis die Verbindungsmodulermittlung abgeschlossen wurde.
Power Denial-Settings (Keine Stromversorgung – Einstellungen)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis die Geräteeinstellungen aktualisiert wurden. Bitte wiederholen Sie den Stromversorgungsvorgang.
Power Denial-Partner Discovery (Keine Stromversorgung – Partnerermittlung)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis die möglichen Partnergeräte ermittelt wurden.
Power Denial-I/O Ready (Keine Stromversorgung – I/O bereit)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis das entsprechende Verbindungsmodul bereit ist.
Power Denial-I/O Missing (Keine Stromversorgung – I/O fehlt)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis das entsprechende Verbindungsmodul in das Gehäuse eingefügt wurde.

Zeile	Beschreibung
Power Denial-SAS Mezz (Keine Stromversorgung – SAS Mezz)	Die Warnung, dass die Gerätestromversorgung verzögert wird, bis die SAS Mezz-Ermittlung abgeschlossen wurde.
Power Denial-Blade Link Discovery (Keine Stromversorgung – Blade-Verbindungsermittlung)	Die Warnung, dass die Gerätestromversorgung während der MMP-Blade-Link-Gerätermittlung verzögert wird.

Informationen zu „Temperature Sensors“ (Temperaturfühler)

Spalte	Beschreibung
Location (Standort)	Ort des Sensors in der Komponente.
Status (Zustand)	Dies ist der Status des Temperatursensors. Der Status entspricht der grafischen Darstellung der Temperatur.
Temperature (Temperatur)	Grafische Darstellung der Temperatur.

iLO

Der iLO-Prozessor für das Server Blade im Komponenteneinschub ist durch Klicken auf **iLO** verfügbar. Die Onboard Administrator-iLO-Seite wird angezeigt, wie im Geräteeinschubs-Abschnitt „iLO Bildschirm“ (iLO-Bildschirm auf Seite 253) beschrieben.

Der Geräteeinschubs-iLO-Bildschirm enthält Links zu mehrere verschiedenen iLO-Schnittstellen. Wenn Sie auf beliebige dieser Links klicken, bietet der Onboard Administrator eine einmalige Anmeldung (Anmeldungsumgehung) bei ProLiant iLO-Verwaltungsprozessoren. Die iLO Zugriffsstufen werden je nach Onboard Administrator-Berechtigungsstufe zugeordnet (Benutzer müssen zum Zugriff auf den Einschub berechtigt sein):

- **Onboard Administrator Administrator** (Administrator von Onboard Administrator): Administer User Accounts (Verwaltung von Benutzerkonten), Remote Console Access (Zugriff auf Remote Console), Virtual Power and Reset (Virtueller Netzschalter und virtuelles Zurücksetzen), Virtual Media (Virtuelle Medien), Configure iLO settings (iLO-Einstellungen konfigurieren).
- **Onboard Administrator Operator** (Bediener von Onboard Administrator): Remote Console Access (Zugriff auf Remote Console), Virtual Power and Reset (Virtueller Netzschalter und virtuelles Zurücksetzen), Virtual Media (Virtuelle Medien).

Ein temporärer iLO Benutzer wird erstellt, wenn ein Onboard Administrator-Benutzer die iLO Weboberfläche oder eine iLO Remote Console startet. Onboard Administrator kann für jeden iLO Prozessor bis zu maximal drei temporäre Konten erstellen. Sind auf einem iLO Prozessor bereits drei oder mehr temporäre Onboard Administrator-Konten vorhanden, löscht Onboard Administrator die ältesten temporären Benutzer in der iLO Benutzerdatenbank.

Port-Zuordnungsinformationen

Port-Zuordnungsinformationen stehen durch Klicken auf **Port Mapping** (Portzuordnung) auf dem Bildschirm „Geräteeinschubs-Informationen“ zur Verfügung.

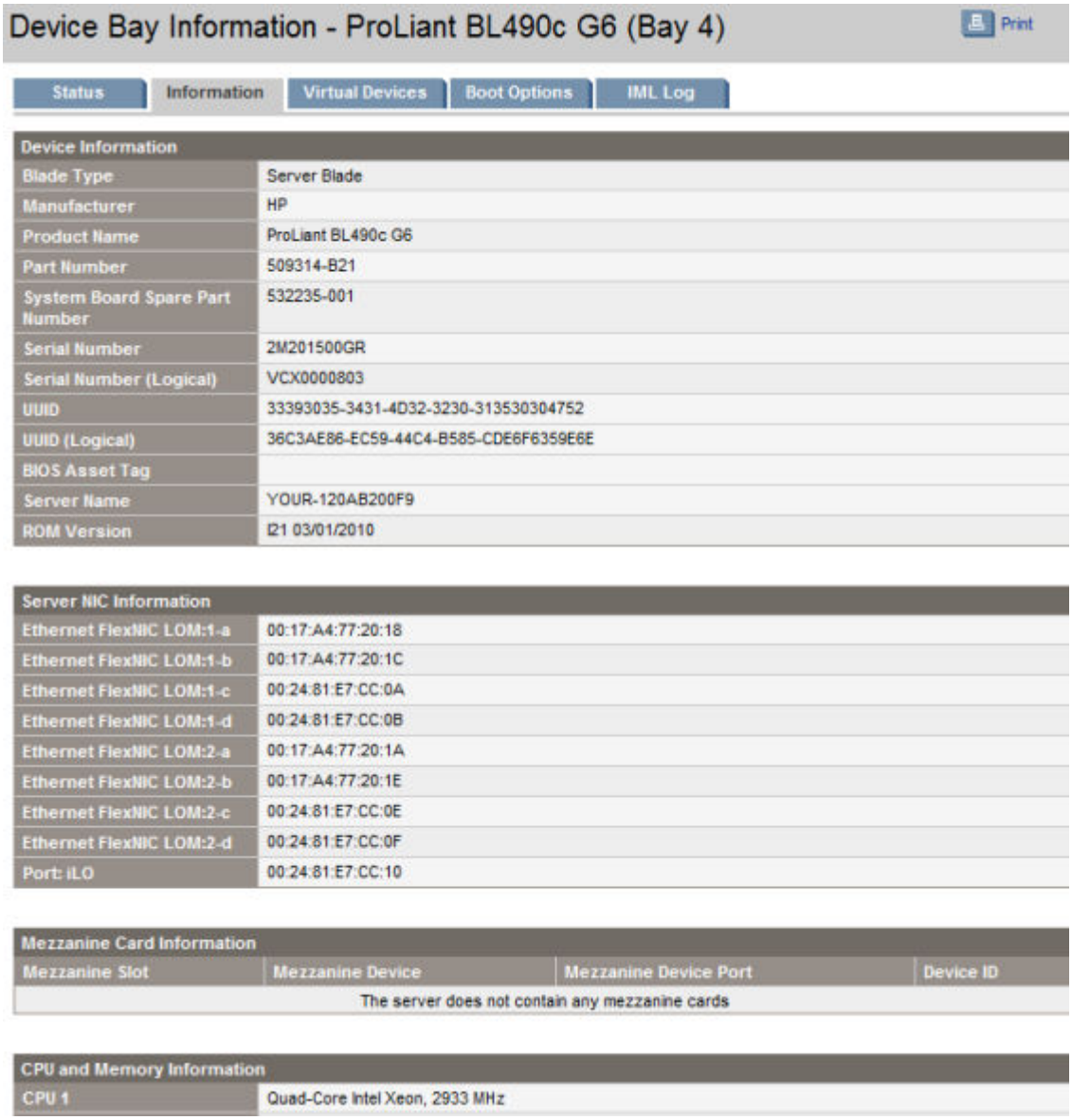
Weitere Informationen finden Sie unter „Portzuordnung“ (Portzuordnung auf Seite 255).

Firmware

Firmware-Informationen zu Geräten im Geräteeinschub sind durch Klicken auf **Firmware** verfügbar.

Weitere Informationen finden Sie unter „Firmware“ (Firmware auf Seite 270).

Registerkarte „Server Blade Information“ (Server Blade-Informationen)



Device Information (Geräteinformationen)

Zeile	Beschreibung
Blade Type (Blade-Typ)	Server Blade
Manufacturer (Hersteller)	Name des Herstellerunternehmens des Server Blade.
Product Name (Produktname)	Allgemeiner beschreibender Name des Server Blade.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatz-Server Blade verwendete Teilenummer
System Board Spare Part Number (Teilenummer der ErsatzSystemplatine)	Die bei der Bestellung einer zusätzlichen oder einer Ersatzsystemplatine verwendete Teilenummer.
Serial Number (Seriennummer)	Die statische Fabrikseriennummer für den Server Blade.

Zeile	Beschreibung
Serial Number (Logical) (Seriennummer (logisch))	Eine logische Seriennummer, die dem Server Blade zugewiesen wurde.
UUID	Die dem Server Blade zugewiesene UUID
UUID (Logical) (UUID (logisch))	Eine dem Server Blade zugewiesene, logische UUID
BIOS Asset Tag (BIOS-Systemkennung)	Die Systemkennung des installierten Server Blade, falls konfiguriert.
Server Name (Servername)	Wurde dieser Name über das BIOS konfiguriert, erscheint er als ProLiant-Servername. Bei ProLiant oder Integrity Server Blades mit installierten HP Betriebssystem-Agenten ist dies der Server-Hostname.*
ROM Version (ROM-Version)	ROM-Versionsnummer.
Boot Mode (Startmodus)	Startmodus für den Server Blade. Der Startmodus wird nur angezeigt, wenn die Unified Extensible Firmware Interface (UEFI) vom Server Blade unterstützt wird. Mögliche Werte sind „Legacy“, „UEFI“ oder „UEFI Optimized“ (UEFI optimiert).
Secure Boot (Sicherer Systemstart)	Status des BIOS-Modus „Secure Boot“ (Sicherer Systemstart) für den Server Blade. Der Status für „Secure Boot“ (Sicherer Systemstart) wird nur angezeigt, wenn der Server Blade im UEFI-Startmodus oder optimierten UEFI-Startmodus konfiguriert ist. Mögliche Werte sind „Enabled“ (Aktiviert) oder „Disabled“ (Deaktiviert). „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich Administratoren) daran, die Standardeinstellungen für Startgeräte zu ändern oder Startvorgänge über die Onboard Administrator-GUI oder -CLI auszuführen. Alle Änderungen an den Starteinstellungen müssen im BIOS vom Administrator vorgenommen werden. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden. „Secure Boot“ (Sicherer Systemstart) wird für Gen8 und frühere Generationen von Server Blades nicht gemeldet. Weitere Informationen zu „Secure Boot“ (Sicherer Systemstart) finden Sie im *HP UEFI System Utilities Benutzerhandbuch* auf der HP Website (http://www.hp.com/go/ProLiantUEFI/docs).

* Über die iLO-Webkonsole können Sie den Servernamen ändern. Die iLO 2-Server verfügen über eine Einschränkung dahingehend, dass der iLO den Onboard Administrator nur dann benachrichtigt, wenn eines der ersten 28 Zeichen des Namens geändert wird. Andernfalls wird keine Benachrichtigung an den Onboard Administrator gesendet. Infolgedessen kann der in Onboard Administrator angezeigte Servername von dem iLO-Server-Namen abweichen.

Server NIC information (Server-NIC-Informationen)

Zeile	Beschreibung
Ethernet FlexNIC LOM:(*x*)-(a-d)	Ein in Virtual Connect konfigurierter Flex-10-fähiger 10 Gb-NIC. Die vier FlexNICs auf Port *x* eines Server LOM, das Flex-10 unterstützt, sind mit LOM:*x*-a, LOM:*x*-b, LOM:*x*-c und LOM:*x*-d nummeriert, wobei *x* für Port 1-4 steht. Einzelheiten zum Konfigurieren von Flex-10-NICs finden Sie im *HP Virtual Connect c-Class BladeSystem Benutzerhandbuch*.
Ethernet FlexNIC LOM: (*y*)-(a-d)	Ein in Virtual Connect konfigurierter Flex-10-fähiger 10 Gb-NIC, wobei x für NIC 1-32 steht. Die vier FlexNICs auf Port *y* eines Server LOM, das Flex-10 unterstützt, sind mit LOM:*y*-a, LOM:*y*-b, LOM:*y*-c und LOM:*y*-d nummeriert, wobei *y* für Port 1-8 steht. Einzelheiten zum Konfigurieren von Flex-10 NICs finden Sie im HP Virtual Connect c-Class BladeSystem Benutzerhandbuch.
Port: NIC *x*	Die MAC-Adresse dieses NIC-Ports, wobei *x* für einen NIC-Port von 1-4 steht.
Port: iLO	Die MAC-Adresse des iLO-Ports für den Server Blade in diesem Gehäusesteckplatz.
Port: iSCSI *x*	Die MAC-Adresse dieses iSCSI -Ports, wobei *x* für einen NIC-Port von 1-8 steht.
Ethernet FCoE FlexFabric Adapter: (*y*)-(a-d)	Ein FCoE FlexFabric Adapter besteht aus 4 NICs. Die vier FlexNICs auf Port *y* eines Server-LOM, das Flex-10 unterstützt, werden folgendermaßen nummeriert: LOM:*y*-a,

Zeile	Beschreibung
	LOM:*y*-b, LOM:*y*-c und LOM:*y*-d, wobei *y* für Port 1–8 steht. LOM:*y*-b kann zur Konfigurierung des FCoE-Datenverkehrs verwendet werden.
Ethernet iSCSI FlexFabric Adapter: (*y*)-(a-d)	Ein iSCSI FlexFabric Adapter besteht aus 4 NICs. Die vier FlexNICs auf Port *y* eines Server-LOM, das Flex-10 unterstützt, werden folgendermaßen nummeriert: LOM:*y*-a, LOM:*y*-b, LOM:*y*-c und LOM:*y*-d, wobei *y* für Port 1–8 steht. LOM:*y*-b kann zur Konfigurierung des iSCSI-Datenverkehrs verwendet werden.

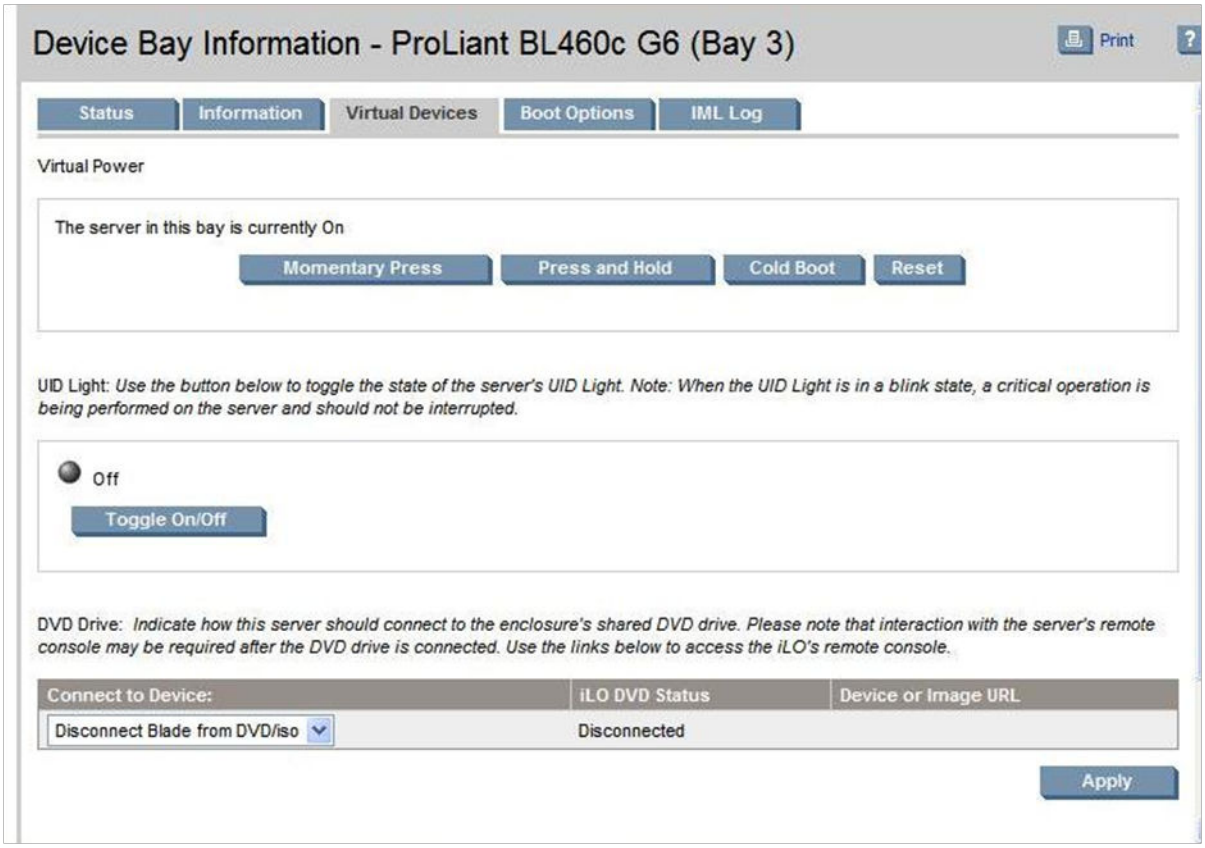
Mezzanine Card Information (Informationen zur Mezzanine Card)

Spalte	Beschreibung
Mezzanine Slot (Mezzanine-Steckplatz)	Der physische Steckplatz, in dem sich die Mezzanine Card befindet.
Mezzanine Device (Mezzanine-Komponente)	Der allgemeine oder Produktname der Mezzanine-Komponenten.
Mezzanine Device Port (Port der Mezzanine-Komponente)	Der Port, der der Mezzanine-Komponente zugewiesen ist.
Device ID (Komponenten-ID)	Die MAC-Adresse des Ports für den Verbindungsmoduleinschub.

CPU and Memory Information (CPU- und Speicherinformationen)

Zeile	Beschreibung
CPU 1 bis CPU (x)	Art von CPU und Geschwindigkeit oder „Not present“ (Nicht vorhanden).
Memory (Arbeitsspeicher)	Speichergröße

Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade)


Device Bay Information - ProLiant BL460c G6 (Bay 3)
Print
Status
Information
Virtual Devices
Boot Options
IML Log
Virtual Power
The server in this bay is currently On
Momentary Press
Press and Hold
Cold Boot
Reset
UID Light: Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critical operation is being performed on the server and should not be interrupted.
Off
Toggle On/Off
DVD Drive: Indicate how this server should connect to the enclosure's shared DVD drive. Please note that interaction with the server's remote console may be required after the DVD drive is connected. Use the links below to access the iLO's remote console.
Connect to Device:
iLO DVD Status
Device or Image URL
Disconnect Blade from DVD/iso
Disconnected
Apply

Virtual Power (Virtueller Netzschalter)

Schaltfläche	Beschreibung
Momentary Press (Kurzes Drücken)	Diese Schaltfläche ahmt ein kurzes physisches Drücken des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade ordnungsgemäß ein- oder ausgeschaltet.
Press and Hold (Rastendes Drücken)	Diese Schaltfläche ahmt ein physisches Drücken und Halten des Netzschalters am Server Blade nach. Bei Anklicken dieser Schaltfläche wird der Server Blade zum Ausschalten gezwungen, ohne zuvor zuerst das Betriebssystem herunterzufahren. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.
Cold Boot (Kaltstart)	Bei Anklicken dieser Schaltfläche wird die Stromversorgung des Systems sofort unterbrochen. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.
Reset (Zurücksetzen)	Bei Anklicken dieser Schaltfläche wird das System zurückgesetzt. Diese Option ist nicht verfügbar, wenn der Server Blade ausgeschaltet ist.

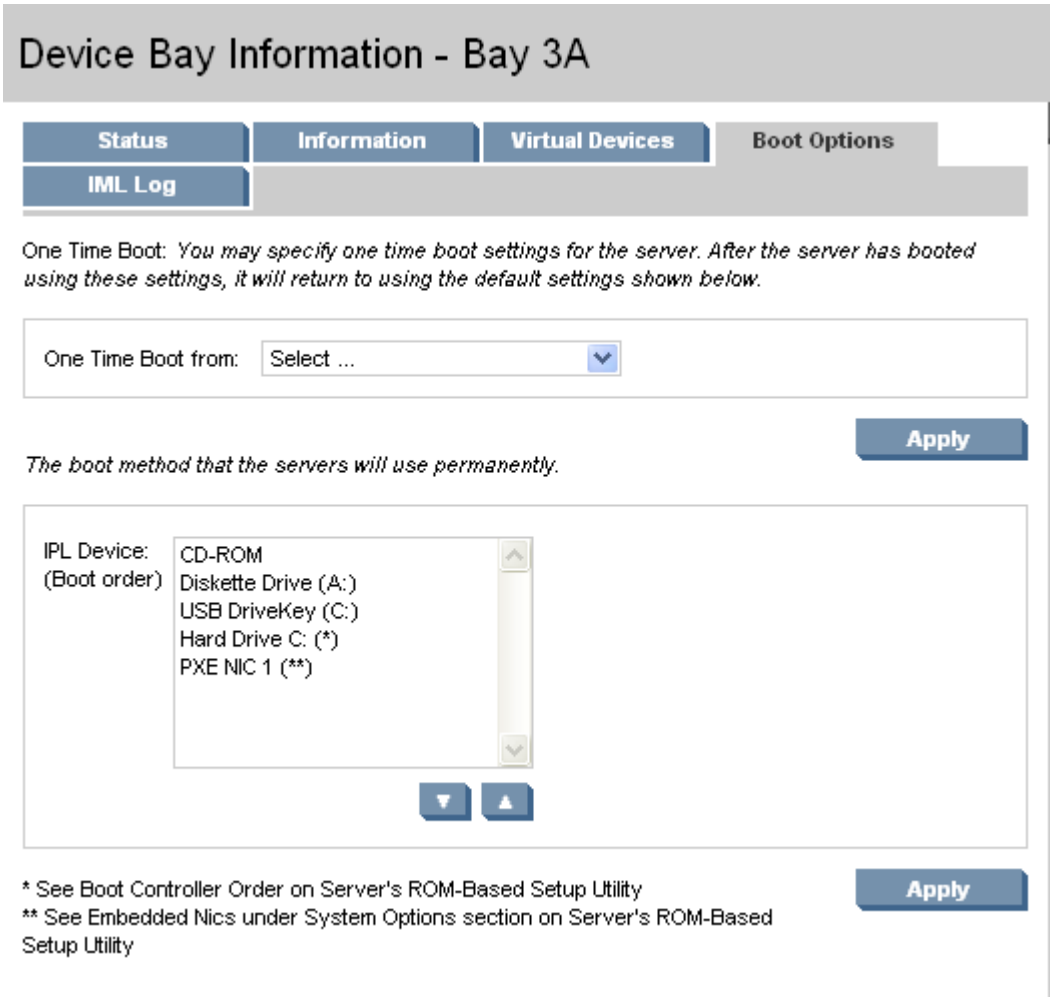
UID Light (UID-LED)

Um einen bestimmten Server Blade zu identifizieren, klicken Sie auf **Toggle On/Off** (Ein-/Ausschalten), um die UID-LED des Server Blade ein- (blau) oder auszuschalten (grau).

DVD Drive (CD/DVD-Laufwerk)

Spalte	Beschreibung
Connect to Device (Mit Komponente verbinden)	Über das Menü können Sie das gemeinsam genutzte DVD-Laufwerk verbinden oder trennen, indem Sie **Connect to Enclosure DVD** (Mit Gehäuse-DVD verbinden) bzw. **Disconnect DVD Hardware** (DVD-Hardware trennen) wählen.
iLO DVD Status (ilO DVD-Status)	Dieses Feld gibt an, ob der Server Blade mit virtuellen Medien verbunden ist. Mögliche Werte sind „Connected“ (Verbunden) oder „Disconnected“ (Getrennt). Lautet der Status „Inkompatible Firmware“, bedeutet dies, dass die DVD-Funktion nicht mit der auf der Komponente installierten iLO Firmware unterstützt wird.
Device or Image URL (Komponente oder Image-URL)	Dieses Feld zeigt die aktuelle virtuelle Medienverbindung des Blades an. Mögliche Werte sind: • Virtual Media Applet is connected (Angeschlossenes Virtual Media Applet) • Feature not supported on Integrity iLO version x.xx (Funktion auf Integrity iLO Version x.xx nicht unterstützt) • SSH is disabled on this blade's iLO processor (SSH ist auf dem iLO-Prozessor dieses Blade deaktiviert) • Upgrade ProLiant iLO version x.xx to 1.30 or higher (ProLiant iLO Version x.xx auf 1.30 oder höher aktualisieren) • Enclosure DVD • Tray Open or No Media (Fach geöffnet oder keine Medien) • URL to USB key ISO image file (URL zu USB-Schlüssel-ISO-Abbilddatei) • ILO has no IP Address (ILO besitzt keine IP-Adresse)

Registerkarte „Boot Options“ (Startoptionen)


Device Bay Information - Bay 3A
Status
Information
Virtual Devices
Boot Options
IML Log
One Time Boot: You may specify one time boot settings for the server. After the server has booted using these settings, it will return to using the default settings shown below.
One Time Boot from:
Select ...
Apply
The boot method that the servers will use permanently.
IPL Device:
(Boot order)
CD-ROM
Diskette Drive (A:)
USB DriveKey (C:)
Hard Drive C: (*)
PXE NIC 1 (**)
* See Boot Controller Order on Server's ROM-Based Setup Utility
** See Embedded Nics under System Options section on Server's ROM-Based Setup Utility
Apply

Einmaliges Booten aus Auswahloptionen

Option	Beschreibung
Select (Auswählen)	Die Standardoption bei der erstmaligen Anzeige oder vor der Vornahme von Änderungen.
Diskette Drive (A:) (Diskettenlaufwerk)	Bewirkt einen Neustart des Server Blade über das Diskettenlaufwerk. Vergewissern Sie sich vor Auswahl dieser Option, dass am Server Blade ein Diskettenlaufwerk angeschlossen ist.
CD-ROM	Bewirkt einen Neustart des Server Blade über das CD-ROM-Laufwerk. Vergewissern Sie sich vor Auswahl dieser Option davon, dass am Server Blade ein CD-ROM-Laufwerk angeschlossen ist.
Hard Drive C: (Festplattenlaufwerk C:)	Bewirkt den Neustart des Server Blade von der Festplatte.
RBSU	Bewirkt das Booten des Server Blade über das RBSU (ROM-Based Setup Utility).
PXE NIC	Bewirkt das Booten des Server Blade über PXE NIC.

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Wenn auf dem Server Blade „Secure Boot“ (Sicherer Systemstart) konfiguriert ist, kann die Option „One Time Boot“ (Einmaliges Starten) nicht ausgewählt werden. Die Option ist abgeblendet. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich Administratoren) daran, diesen Vorgang über die Onboard Administrator-GUI oder -CLI auszuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

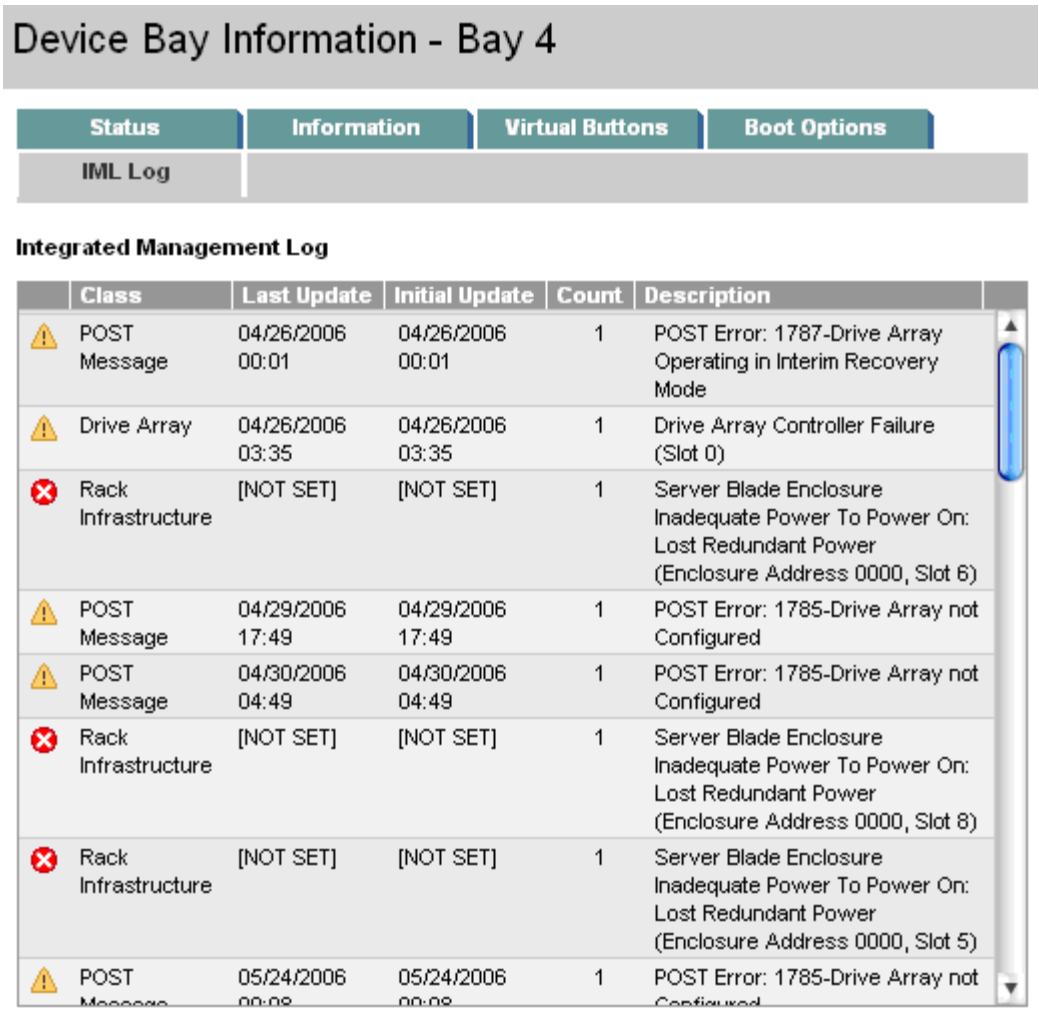
Standard Boot Order (IPL) (IPL-Standard-Boot-Reihenfolge)

Wählen Sie zur Festlegung einer Standard-Boot-Reihenfolge in der Liste „Boot order“ (Boot-Reihenfolge) eine Komponente aus, und verschieben Sie die Boot-Komponente mithilfe des Nach-oben-Pfeils bzw. Nach-unten-Pfeils. Setzen Sie diesen Vorgang fort, bis Sie die Komponenten in der gewünschten Reihenfolge angeordnet haben. Alternativ können Sie die Standard-Boot-Reihenfolge über RBSU festlegen. Alle Neustarts verwenden die Boot-Reihenfolge, die in den Einstellungen für die Standard-Boot-Reihenfolge angegeben ist, sofern nicht die einmalige Boot-Option gewählt wurde.

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

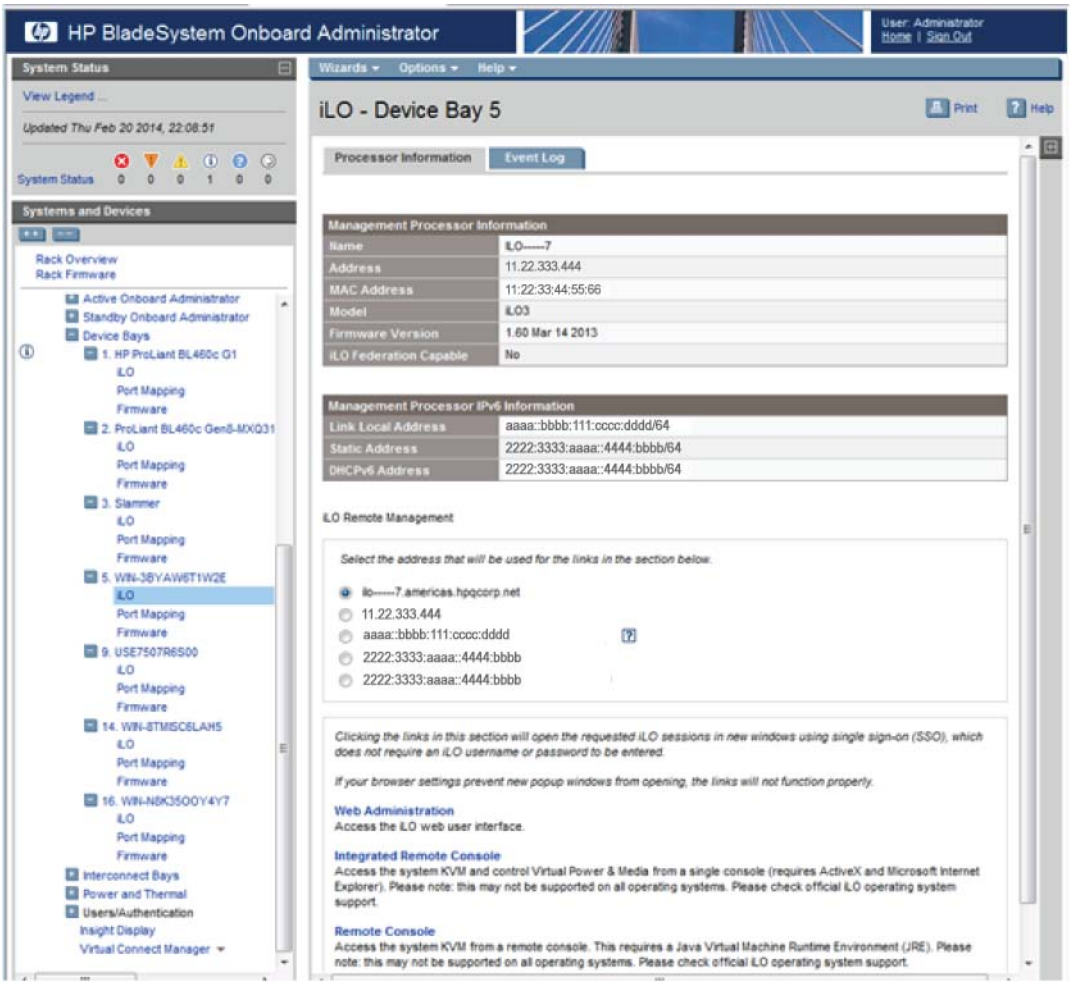
Wenn auf dem Server Blade „Secure Boot“ (Sicherer Systemstart) konfiguriert ist, können die IPL-Geräte nicht ausgewählt werden. Die Geräteliste ist abgeblendet. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich Administratoren) daran, diesen Vorgang über die Onboard Administrator-GUI oder -CLI auszuführen. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Registerkarte „IML Log“



Auf der Registerkarte „IML Log“ (IML-Protokoll) werden die Informationen angezeigt, die im IML des Server Blade gespeichert wurden. Die Protokolleinträge können Informations-, Warn- oder kritische Zustände enthalten. Die Spalten „Last Update“ (Letzte Aktualisierung) und „Initial Update“ (Erste Aktualisierung) enthalten Zeitangaben, und die Spalte „Count“ (Anzahl) zeigt an, wie häufig der Eintrag protokolliert wurde. Die Spalte „Description“ (Beschreibung) enthält den vollständigen Eintrag mit einer ausführlicheren Beschreibung.

iLO-Bildschirm



Die in diesem Bildschirm angezeigten Informationen umfassen die Registerkarten „Processor Information“ (Prozessordaten), „Processor IPv6 Information“ (Prozessor-IPv6-Daten) und „Event Log“ (Ereignisprotokoll). Klicken Sie zum Anzeigen der Vorder- und der Rückansicht des Geräteeinschubs auf die Schaltfläche **Left Arrow** (Linker Pfeil) in der rechten oberen Bildschirmecke.

Registerkarte „Processor Information“ (Prozessordaten)

Zeile	Beschreibung
Name	Der DNS-Name des iLO Prozessors.
Address (Adresse)	Die IP-Adresse des iLO Prozessors.
MAC Address (SLAAC-Adresse)	Die MAC-Adresse des iLO Prozessors.
Model (Modell)	Die allgemeine Beschreibung des iLO Prozessors.
Firmware Version (Firmwareversion)	Die zu installierende Firmwareversion des iLO Prozessors.
VLAN ID (Name)	Die VLAN-ID-Nummer und der VLAN-Name des Geräteeinschubs, wenn VLAN aktiviert ist.
iLO Federation Capable (iLO Federation-fähig)	Gibt an, ob der Server Blade zur Unterstützung von iLO Federation fähig ist. Dies bedeutet nur, dass iLO zur Teilnahme an iLO Federation konfiguriert werden kann. Hiermit wird nicht angegeben, ob iLO derzeit für die tatsächliche Teilnahme an

Zeile	Beschreibung
	iLO Federation konfiguriert ist. Zur vollständigen Aktivierung von iLO Federation muss „Enclosure iLO Federation Support“ (Unterstützung für Gehäuse-iLO Federation) auf dem Onboard Administrator aktiviert sein (weitere Informationen finden Sie auf der Seite „Network Access“ (Netzwerkzugriff). Außerdem muss jeder iLO über die entsprechende Firmware verfügen und zum Unterstützen von iLO Federation konfiguriert sein (weitere Informationen finden Sie im *HP iLO 4 Benutzerhandbuch* auf der HP Website (http://www.hp.com/go/ilo/docs)).

Registerkarte „Processor IPv6 Information“ (Prozessor-IPv6-Daten)

Zeile	Beschreibung
Link Local Address (Lokale Verbindungsadresse)	Die lokale IPv6-Verbindungsadresse des iLO Prozessors
Static Address (Statische Adresse)	Die statische IPv6-Adresse des iLO Prozessors
EBIPA Address (EBIPA-Adresse)	Die EBIPA-IPv6-Adresse des iLO Prozessors
DHCPv6 Address (DHCPv6-Adresse)	Die DHCP-IPv6-Adresse des iLO Prozessors
SLAAC Address (SLAAC-Adresse)	Die SLAAC-IPv6-Adresse des iLO Prozessors

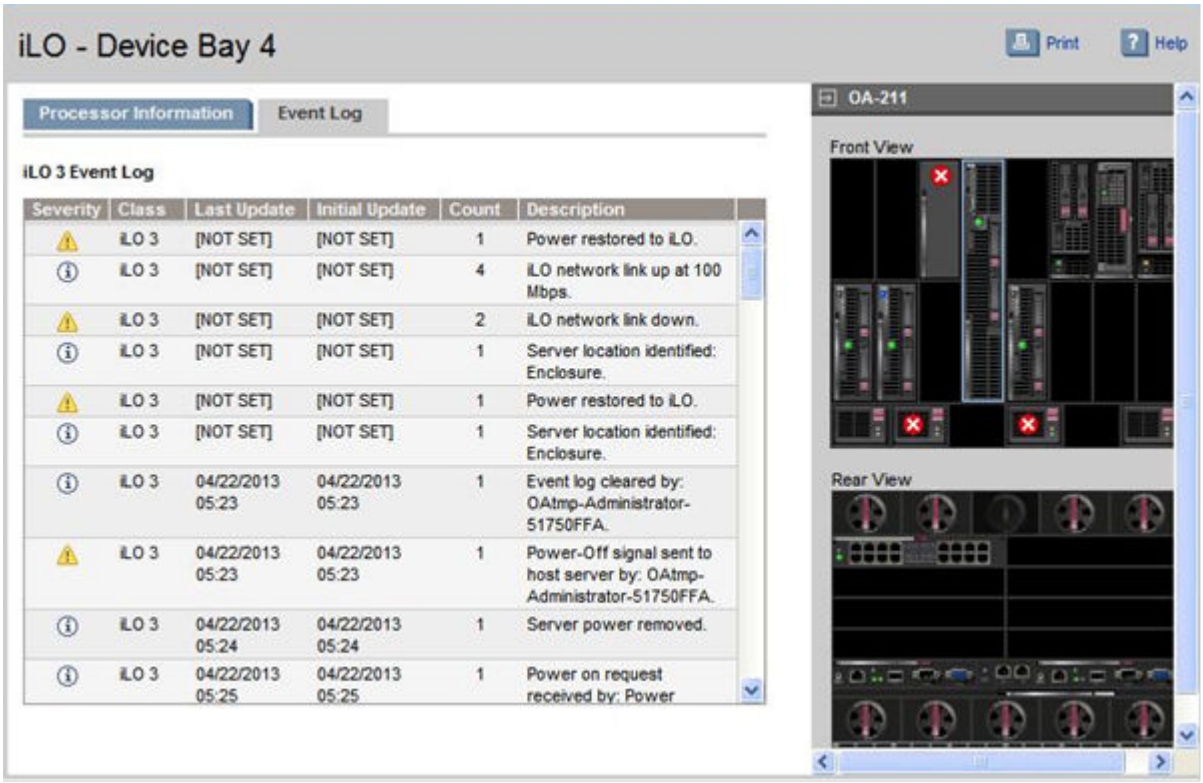
iLO Remote-Management

In diesem Bereich befinden sich Links zu den angeforderten iLO Sitzungen.

Wenn das IPv6-Protokoll oder die FQDN-Link-Unterstützung aktiviert ist, erscheint ein IP-Adressen-Gruppenfeld. Dieses Gruppenfeld ermöglicht die Auswahl der IP-Adresse, die für Links verwendet werden soll, mit denen auf die iLO-Sitzungen zugegriffen wird. Wenn die FQDN-Link-Unterstützung aktiviert ist und bestimmte DNS-Konfigurationsvoraussetzungen erfüllt sind, ist eine FQDN-basierte-Adresse die Standardvorgabe. Weitere Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).

Wenn eine Funktion mit erforderlicher Popup-Fenster-Unterstützung nicht richtig funktioniert, stellen Sie sicher, dass das Öffnen von Popup-Fenstern nicht durch die Browser-Einstellungen verhindert wird. Informationen zum Ausschalten von Popup-Fenster-Blockern finden Sie in den spezifischen Onlinehilfedateien Ihres Browsers.

Registerkarte „iLO Event Log“ (iLO-Ereignisprotokoll)


iLO - Device Bay 4
Print
Help
Processor Information
Event Log
iLO 3 Event Log
Severity
Class
Last Update
Initial Update
Count
Description
iLO 3 [NOT SET] [NOT SET] 1 Power restored to iLO.
iLO 3 [NOT SET] [NOT SET] 4 iLO network link up at 100 Mbps.
iLO 3 [NOT SET] [NOT SET] 2 iLO network link down.
iLO 3 [NOT SET] [NOT SET] 1 Server location identified: Enclosure.
iLO 3 [NOT SET] [NOT SET] 1 Power restored to iLO.
iLO 3 [NOT SET] [NOT SET] 1 Server location identified: Enclosure.
iLO 3 04/22/2013 05:23 04/22/2013 05:23 1 Event log cleared by: OAtmp-Administrator-51750FFA.
iLO 3 04/22/2013 05:23 04/22/2013 05:23 1 Power-Off signal sent to host server by: OAtmp-Administrator-51750FFA.
iLO 3 04/22/2013 05:24 04/22/2013 05:24 1 Server power removed.
iLO 3 04/22/2013 05:25 04/22/2013 05:25 1 Power on request received by: Power
OA-211
Front View
Rear View

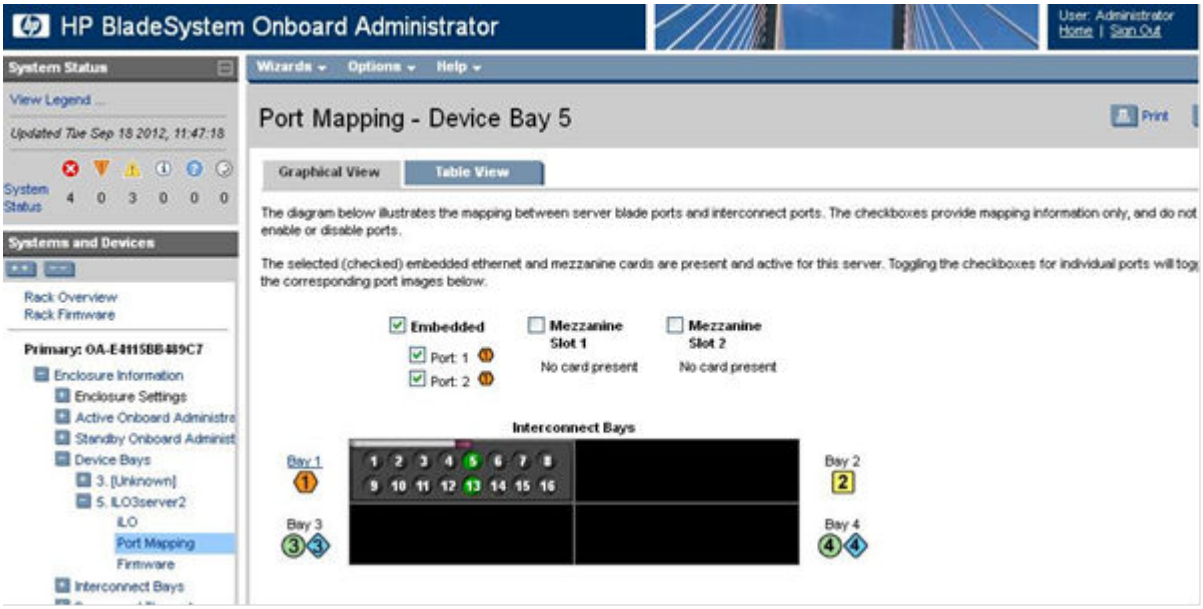
Diese Registerkarte zeigt die Informationen des iLO-Ereignisprotokolls von iLO an. Es kann nicht in der grafischen Benutzeroberfläche von Onboard Administrator bearbeitet werden. Ausführliche Informationen zum iLO-Ereignisprotokoll finden Sie in der iLO-Dokumentation.

Portzuordnung

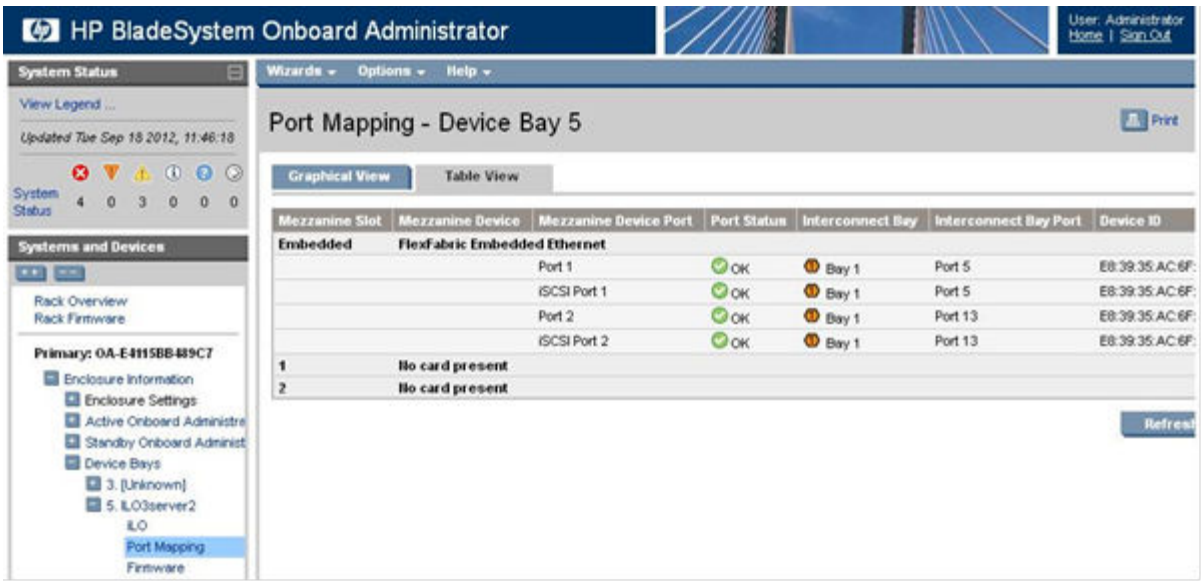
Der Bildschirm „Port Mapping“ (Portzuordnung) erscheint, wenn Sie im Bildschirm „Device Bay Informationen“ (Geräteeinschubs-Informationen) auf **Port Mapping Information** (Portzuordnungs-Informationen) klicken.

Die folgenden zwei Bildschirme zeigen Beispiele der Portzuordnungs-Registerkarten **Graphical View** (Grafische Ansicht) und **Table View** (Tabellenansicht).

Grafische Ansicht



Tabellenansicht

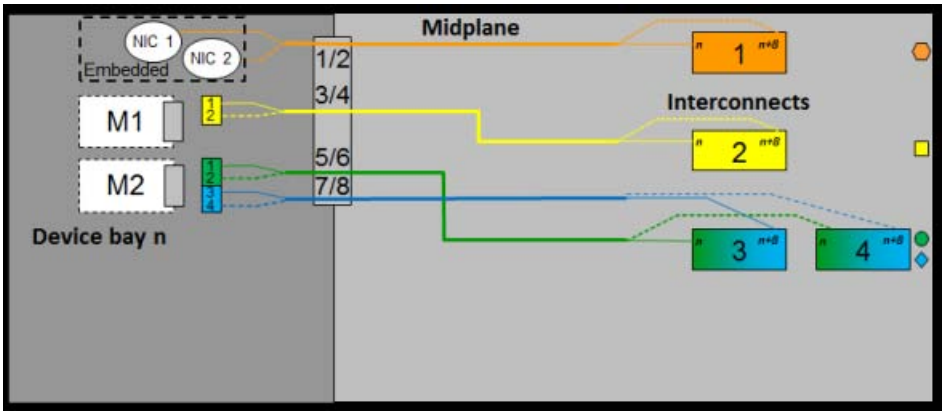


Weitere Informationen finden Sie in den folgenden Abschnitten in diesem Dokument. Beziehen Sie sich zudem auf die neueste Dokumentation für das c3000-Gehäuse und c7000-Gehäuse in der HP BladeSystem-Informationsbibliothek (http://www.hp.com/support/BladeSystem/docs).

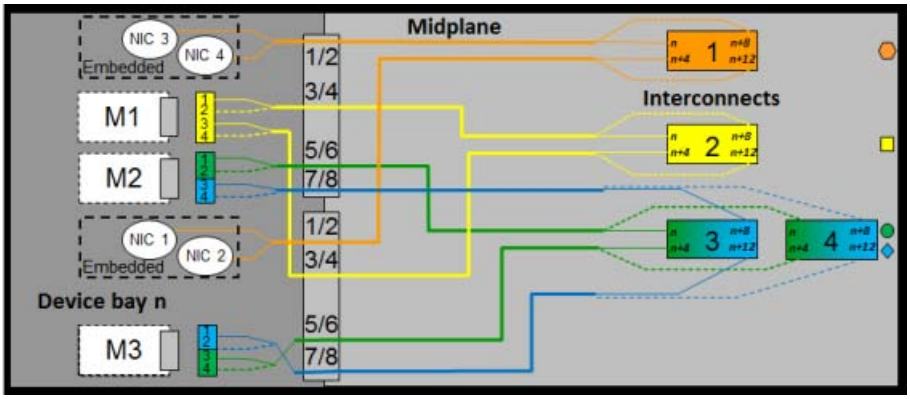
- „Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse (Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse auf Seite 257)“
- „Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse (Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse auf Seite 259)“
- „Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse (Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse auf Seite 263)“
- „Tabellenansicht der Portzuordnungen der Geräteeinschübe für das c7000-Gehäuse (Tabellenansicht der Portzuordnungen der Geräteeinschübe für das c7000-Gehäuse auf Seite 266)“

Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse

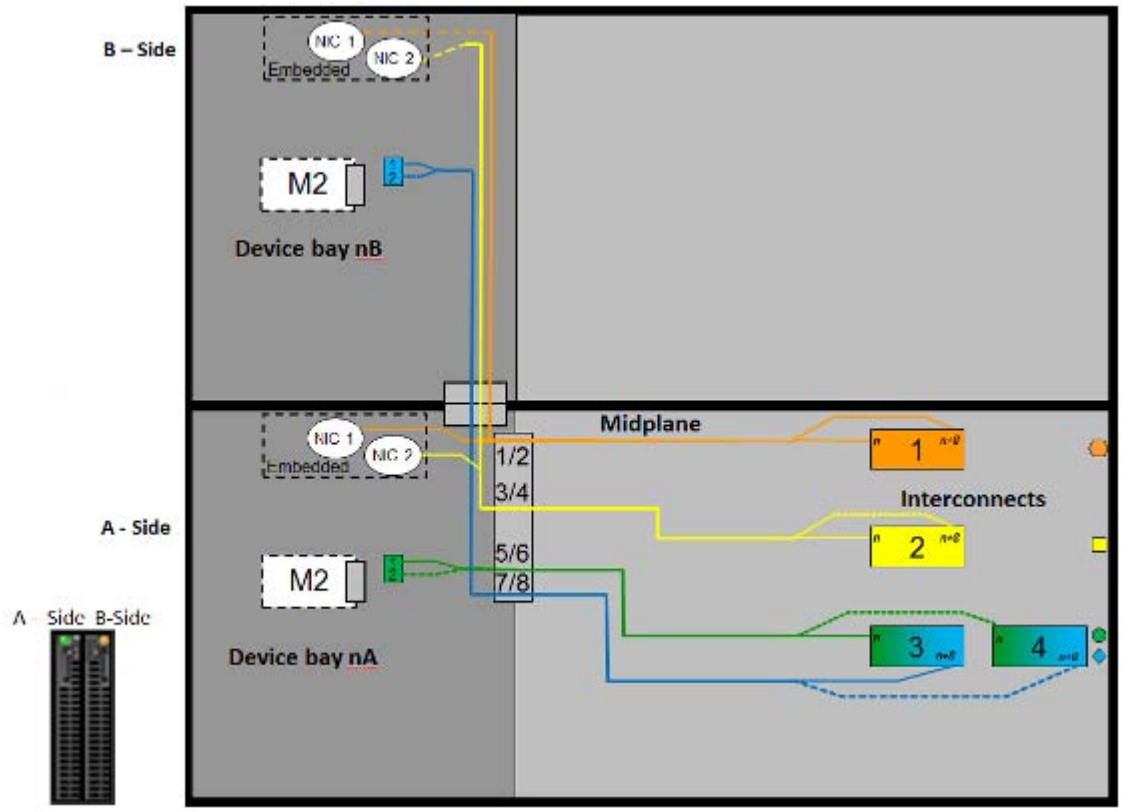
Server Blades halber Höhe und einfacher Breite (wie z. B. HP ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c und WS460c)



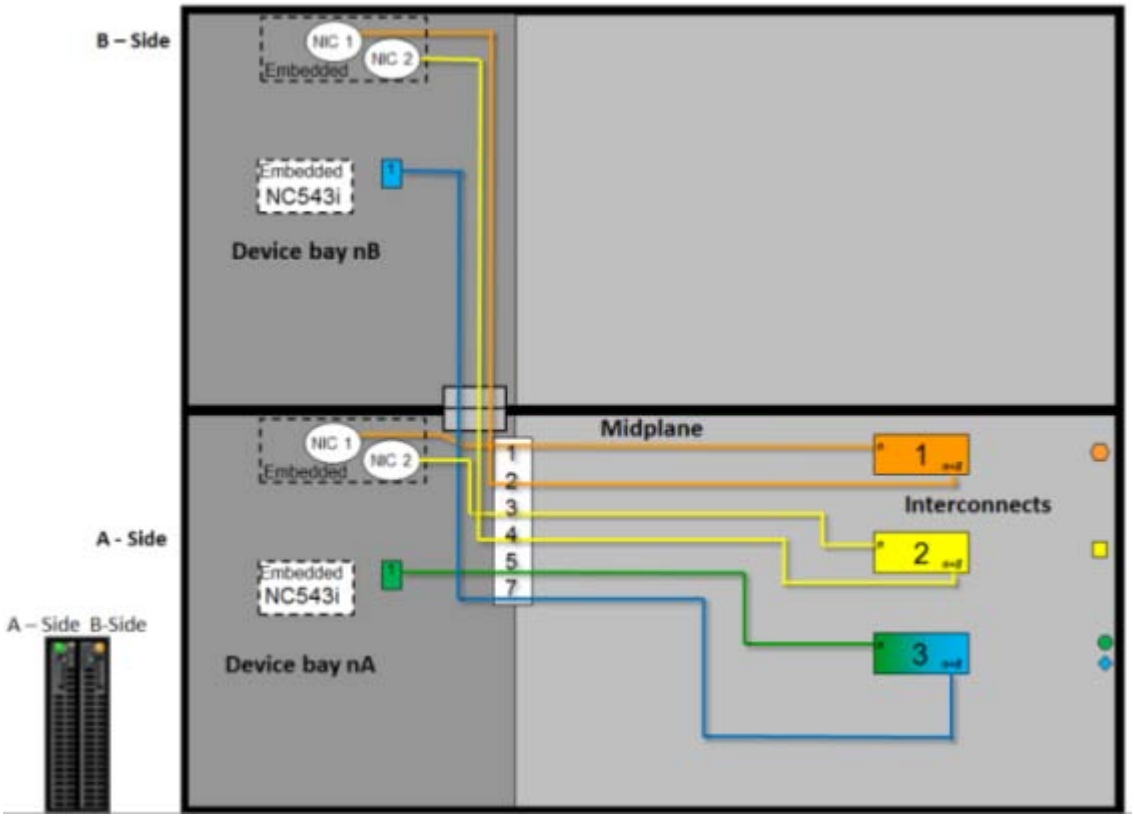
Server Blades halber Höhe und einfacher Breite (wie z. B. HP ProLiant BL680c (G1), BL680c Gen5 und BL480c, BL620c, BL660c und BL685c)



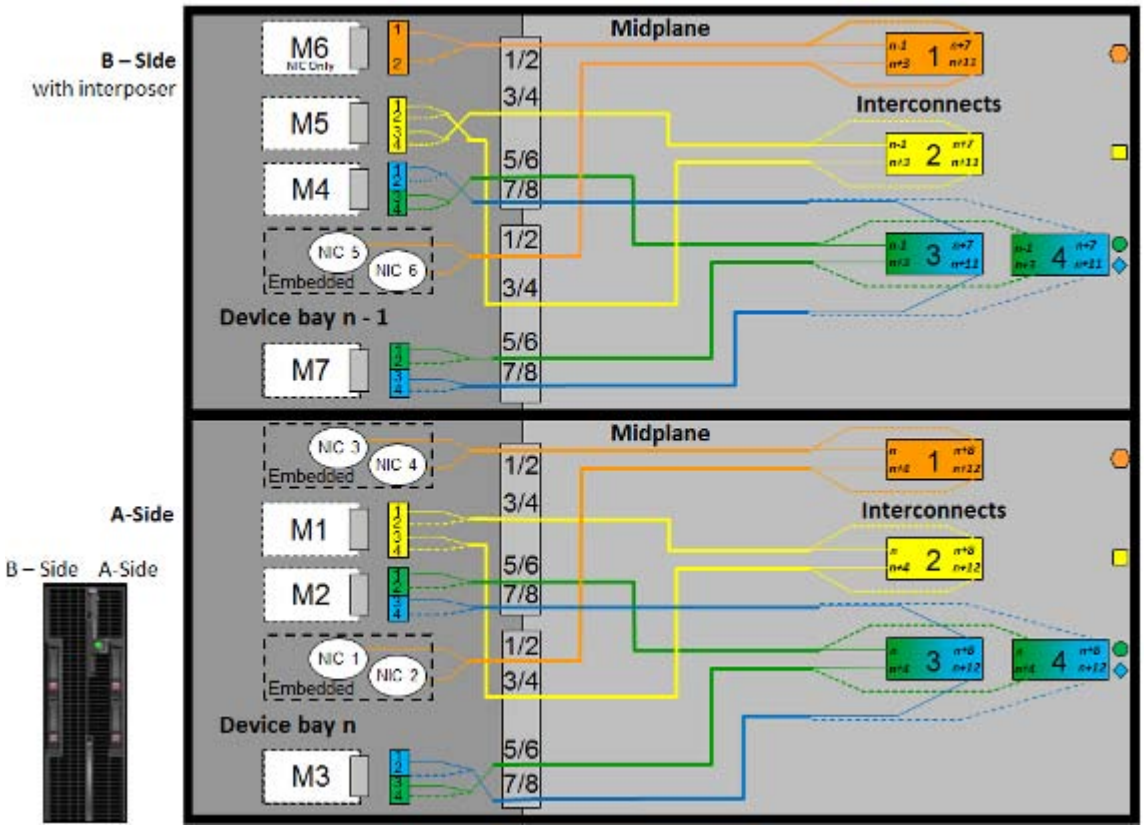
Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c (G1)–G6)



Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c G7



Server Blades voller Höhe und doppelter Breite wie z. B. HP ProLiant BL680c G7



Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse

Die Server Blades werden den Verbindungsmoduleinschüben folgendermaßen zugeordnet. Die Begriffe „1x“, „2x“ oder „4x“ beziehen sich auf die Anzahl von Verbindungsleitungen pro Port, die vom Controller bereitgestellt werden. Wenn ein Gerät nicht vorhanden ist, ist das Kontrollkästchen deaktiviert und der Port kann nicht angezeigt werden.

- Beispiele für 1x-Ports sind 1 GB Ethernet (1 GbE), 10 GB Ethernet (10 GbE) und alle Fibre Channel-Geräte.
- Beispiele für 2x-Ports sind 20 GB Ethernet (20 GbE) und alle seriell angeschlossenen SCSI (SAS)-Geräte.
- Beispiele für 4x-Ports sind alle InfiniBand-Geräte.
- In den folgenden Tabellen werden die Ethernet-Ports als NICs bezeichnet.

HINWEIS: 1x- und 2x-Port-Mezzanine Cards kommunizieren mit Verbindungsmodulen einfacher Breite. 4x-Port-Mezzanine Cards kommunizieren mit Verbindungsmodulen doppelter Breite.

Server Blades halber Höhe und einfacher Breite

Die folgende Tabelle listet die Portzuordnung der in einem c3000-Geräteeinschub N (1–8) halber Höhe installierten Server Blades halber Höhe auf. Beispiele für solche Server Blades halber Höhe sind HP ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c und WS460c.

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
NIC *	NIC 1 (Port:1) NIC 2 (Port:2)	1/Port N 1/Port N+8	Ein Ethernet-Verbindungsmodul einfacher Breite
Mezzanine-Steckplatz 1: 1x- oder 2x-Karten (4x-Karten werden von diesem Steckplatz nicht unterstützt)	1x-/2x-Port 1 1x-/2x-Port 2	2/Port N 2/Port N+8	• Ein Verbindungsmodul einfacher Breite • Nur zwei Ports werden verbunden. • Vier Port-Karten, wobei nur eine Verbindung zu den ersten beiden Ports hergestellt wird.
Mezzanine-Steckplatz 2: 1x- oder 2x-Karten	1x-/2x-Port 1 1x-/2x-Port 2 1x-/2x-Port 3 1x-/2x-Port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8	Ein oder zwei Verbindungsmodule einfacher Breite
Mezzanine-Steckplatz 2: 4x-Karten	4x-Port 1 4x-Port 2	3/Port N 3/Port N+8	Ein Verbindungsmodul doppelter Breite

* G7 und frühere Generationen von Server Blades verfügen über auf der Systemplatine integrierte Ethernet-Ports. Bei Server Blades ab Gen8 befinden sich die Ethernet-Ports auf einer vom Benutzer auswählbaren Karte, die als FlexibleLOM-Adapter bezeichnet wird. Für die Ports des FlexibleLOM-Adapters und für die integrierten Netzwerkadapter-Ports gilt die gleiche Zuordnung.

Server Blades voller Höhe und einfacher Breite

Die folgende Tabelle listet die Portzuordnung der in einem c3000-Geräteeinschub N (1–4) voller Höhe installierten Server Blades voller Höhe und einfacher Breite auf. Beispiele für solche Server Blades voller Höhe sind HP ProLiant BL680c (G1), BL680c Gen5 und BL480c, BL620c, BL660c und BL685c.

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
NIC*	NIC 1 (Port:1) NIC 2 (Port:2) NIC 3 (Port:3) NIC 4 (Port:4)	1/Port N+4 1/Port N+12 1/Port N 1/Port N+8	Ein Ethernet-Verbindungsmodul einfacher Breite
Mezzanine-Steckplatz 1: 1x- oder 2x-Karten (4x-Karten werden von diesem Steckplatz nicht unterstützt)	1x-/2x-Port 1 1x-/2x-Port 2 1x-/2x-Port 3 1x-/2x-Port 4	2/Port N 2/Port N 2/Port N+4 2/Port N+12	Ein Verbindungsmodul einfacher Breite
Mezzanine-Steckplatz 2: 1x- oder 2x-Karten	1x-/2x-Port 1 1x-/2x-Port 2	3/Port N 4/Port N	Ein oder zwei Verbindungsmodule einfacher Breite

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
	1x-/2x-Port 3	3/Port N+8	
	1x-/2x-Port 4	4/Port N+8	
Mezzanine-Steckplatz 2: 4x-Karten	4x-Port 1	3/Port N	Ein Verbindungsmodul doppelter Breite
	4x-Port 2	3/Port N+8	
Mezzanine-Steckplatz 3: 1x- oder 2x-Karten	1x-/2x-Port 1	3/Port N+12	Ein oder zwei Verbindungsmodule einfacher Breite
	1x-/2x-Port 2	4/Port N+12	
	1x-/2x-Port 3	3/Port N+4	
	1x-/2x-Port 4	4/Port N+4	
Mezzanine-Steckplatz 3: 4x-Karten	4x-Port 1	3/Port N+12	Ein Verbindungsmodul doppelter Breite
	4x-Port 2	3/Port N+4	

* G7 und frühere Generationen von Server Blades verfügen über auf der Systemplatine integrierte Ethernet-Ports. Bei Server Blades ab Gen8 befinden sich die Ethernet-Ports auf einer vom Benutzer auswählbaren Karte, die als FlexibleLOM-Adapter bezeichnet wird. Für die Ports des FlexibleLOM-Adapters und für die integrierten Netzwerkadapter-Ports gilt die gleiche Zuordnung.

Server Blades halber Höhe und doppelter Dichte

In der folgenden Tabelle werden die verfügbaren Konfigurationen für die in einem c3000-Geräteeinschub N (1–8) halber Höhe installierten Server Blades doppelter Dichte aufgeführt. Beispiele für diese Server Blades doppelter Dichte sind HP ProLiant BL2x220c (G1) – G6.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC von Server A	NIC 1 (Port:1)	1/Port N
	NIC 2 (Port:2)	2/Port N
Mezzanine von Server A	Port 1	3/Port N
	Port 2	4/Port N
Integrierter NIC von Server B	NIC 1 (Port:1)	1/Port N+8
	NIC 2 (Port:2)	2/Port N+8
Mezzanin von Server B	Port 1	3/Port N+8
	Port 2	4/Port N+8

Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c G7

In der folgenden Tabelle werden die verfügbaren Konfigurationen für in einem c3000-Geräteeinschub N (1–8) halber Höhe installierte Geräte doppelter Dichte, wie z. B. HP ProLiant BL2x220c G7, aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC von Server A	NIC 1 (Port:1)	1/Port N
	NIC 2 (Port:2)	2/Port N

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Server A NC543i*	Port 1	3/Port N
Integrierter NIC von Server B	NIC 1 (Port:1)	1/Port N+8
	NIC 2 (Port:2)	2/Port N+8
Server B NC543i*	Port 1	3/Port N+8

* Der im HP ProLiant BL2x220c G7 Server Blade integrierte NC543i wird automatisch von Onboard Administrator für Ethernet konfiguriert, wenn in Einschub 3 ein Ethernet-Verbindungsmodul installiert ist, oder für InfiniBand, wenn in Einschub 3 ein InfiniBand-Verbindungsmodul doppelter Breite installiert ist. Um die NC543i-Konfiguration zum jeweils anderen Typ zu ändern, schalten Sie alle HP ProLiant BL2x220c G7 Server Blades aus, und ersetzen Sie das Verbindungsmodul durch den jeweils anderen Typ. Wenn Sie das aktive Onboard Administrator-Modul neu starten oder alle HP ProLiant BL2x220c G7 Server Blades erneut einstecken, dann konfiguriert der Onboard Administrator alle integrierten NC543i-Geräte entsprechend des neuen Verbindungstyps neu.

AMC Telco I/O-Erweiterungs-Blade

In der Tabelle werden die verfügbaren Konfigurationen für die in einem c3000-Geräteeinschub N (1–8) halber Höhe installierten AMC Telco-Geräte aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
AMC integriert (1)	Port 1	1/Port N
	Port 3	2/Port N
AMC integriert (2)	Port 5	3/Port N
	Port 7	4/Port N

Server Blades voller Höhe und doppelter Breite wie z. B. HP ProLiant BL680c G7

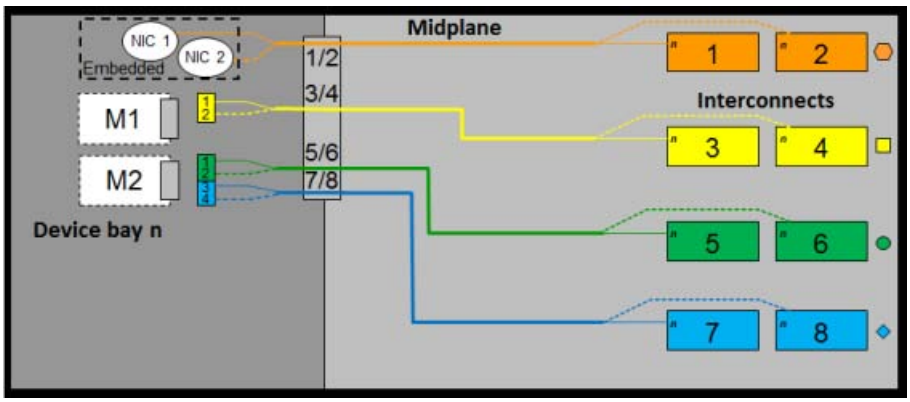
In der folgenden Tabelle werden die verfügbaren Konfigurationen für die in einem c3000-Geräteinschub N (2 oder 4) installierten Server Blades voller Höhe und doppelter Breite, wie z. B. HP ProLiant BL2x220c G7, aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC auf Seite A	NIC 1	1/Port N+4
	NIC 2	1/Port N+12
	NIC 3	1/Port N
	NIC 4	1 Port N+8
Integrierter NIC auf Seite B	NIC 5	1/Port N+3
	NIC 6	2/Port N+11
Mezzanine 1 auf Seite A	Port 1	2/Port N
	Port 2	2/Port N+8
	Port 3	2/Port N+4
	Port 4	2/Port N+12
Mezzanine 2 auf Seite A	Port 1	3/Port N
	Port 2	4/Port N

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
	Port 3	3/Port N+8
	Port 4	4/Port N+8
Mezzanine 3 auf Seite A	Port 1	3/Port N+12
	Port 2	4/Port N+12
	Port 3	3/Port N+4
	Port 4	4/Port N+4
Mezzanine 4 auf Seite B	Port 1	3/Port N+7
	Port 2	4/Port N+7
	Port 3	2/Port N-1
	Port 4	2/Port N-1
Mezzanine 5 auf Seite B	Port 1	2/Port N+3
	Port 2	2/Port N+11
	Port 3	2/Port N-1
	Port 4	2/Port N+7
Mezzanine 6 auf Seite B	Port 1	1/Port N-1
Nur NIC	Port 2	1/Port N+7
Mezzanine 7 auf Seite B	Port 1	3/Port N+3
	Port 2	4/Port N+3
	Port 3	3/Port N+11
	Port 4	4/Port N+11

Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse

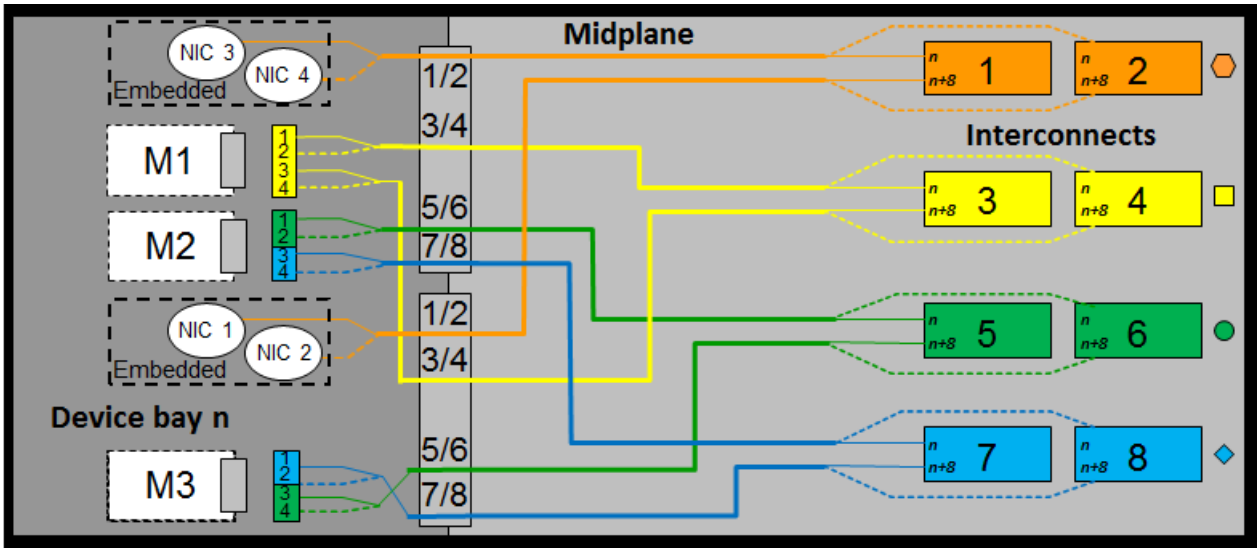
Server Blades halber Höhe und einfacher Breite (wie z. B. HP ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c und WS460c)



In diesem Diagramm entspricht N der Nummer des Server Blade im Gehäuse und der Portnummer auf dem Switch. Wenn Sie z. B. ein Server Blade in Steckplatz 1 einsetzen, wird es als Komponente 1 angesehen, und die Ports, die in Switch 1 und Switch 2 verwendet werden, sind Ports 1 bzw. Ports 2. Wenn Sie ein Server Blade in Steckplatz 2 einsetzen, dann sind die Ports, die auf Switch 1 und

2 verwendet werden, die Ports 2 und 2. Diese Konvention ändert sich für Server Blades mit voller Bauhöhe, wie im nächsten Diagramm zu sehen ist.

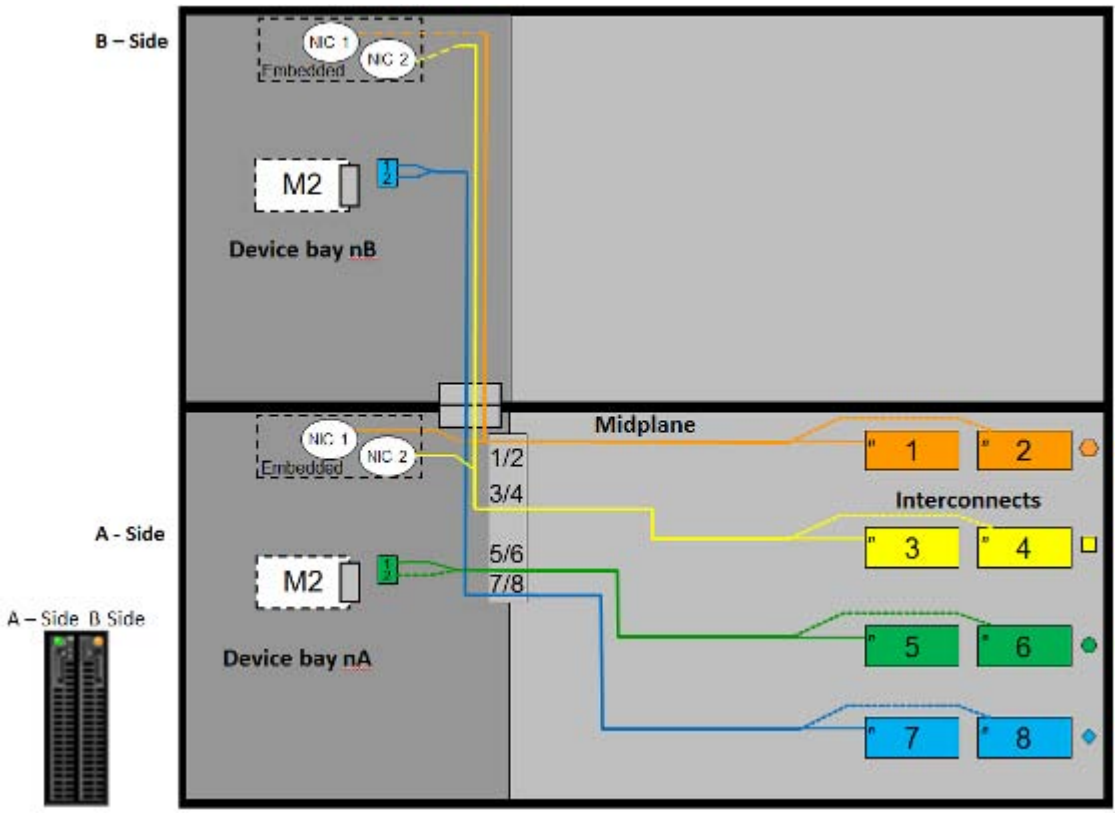
Server Blades voller Höhe und einfacher Breite (wie z. B. HP ProLiant BL680c (G1), BL680c Gen5 und BL480c, BL620c, BL660c und BL685c)



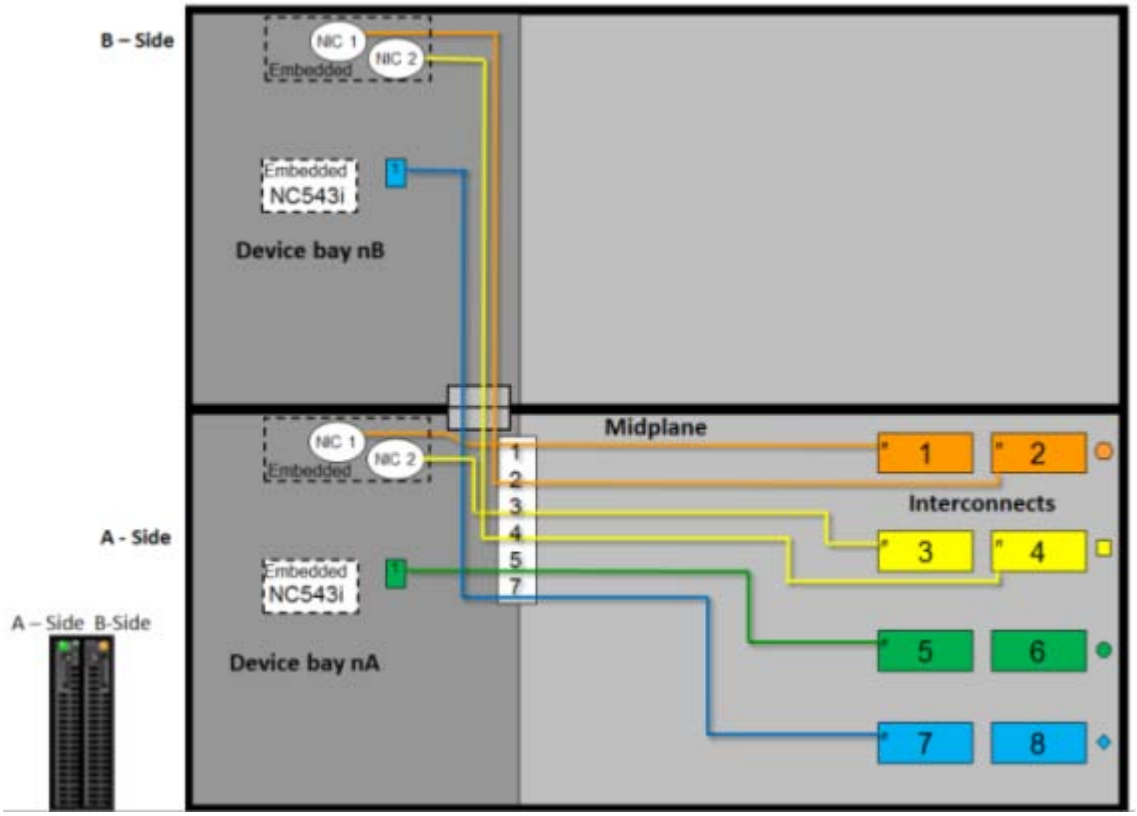
In diesem Diagramm entspricht N der Nummer des Blade im Gehäuse und der Portnummer für den Switch. Wenn Sie z. B. ein Blade in Steckplatz 1 einsetzen, wird es als Komponente 1 angesehen. Da Server Blades voller Höhe und einfacher Breite den Platz von zwei Server Blades halber Höhe einnehmen, ist das Gehäuse auf maximal acht Server Blades mit voller Bauhöhe und einfacher Breite eingeschränkt. Die Portzuordnung dieser Server Blades voller Höhe und einfacher Breite scheint sich anfänglich von der von Server Blades halber Höhe zu unterscheiden, sie verwenden jedoch sehr ähnliche Konventionen.

Wie bei einem Server Blade mit halber Bauhöhe gilt: Wenn Sie ein Blade in Steckplatz 1 einfügen, wird es als Komponente 1 angesehen. Jedoch verfügt es über eine zweite Gruppe von Ports, die ebenfalls Switches 1 und 2 zugeordnet werden. Bei Server Blades voller Höhe und einfacher Breite wird ein N/N+8-Schema auf den Switches verwendet. Aus diesem Grund wird Server Blade 1 den Ports 1 und 9 auf beiden Switches zugeordnet, da N=1 Wenn Sie ein Server Blade in Steckplatz 2 einsetzen, dann sind die vier Ports auf Switches 1 und 2 die Ports 2 und 10, da N=2.

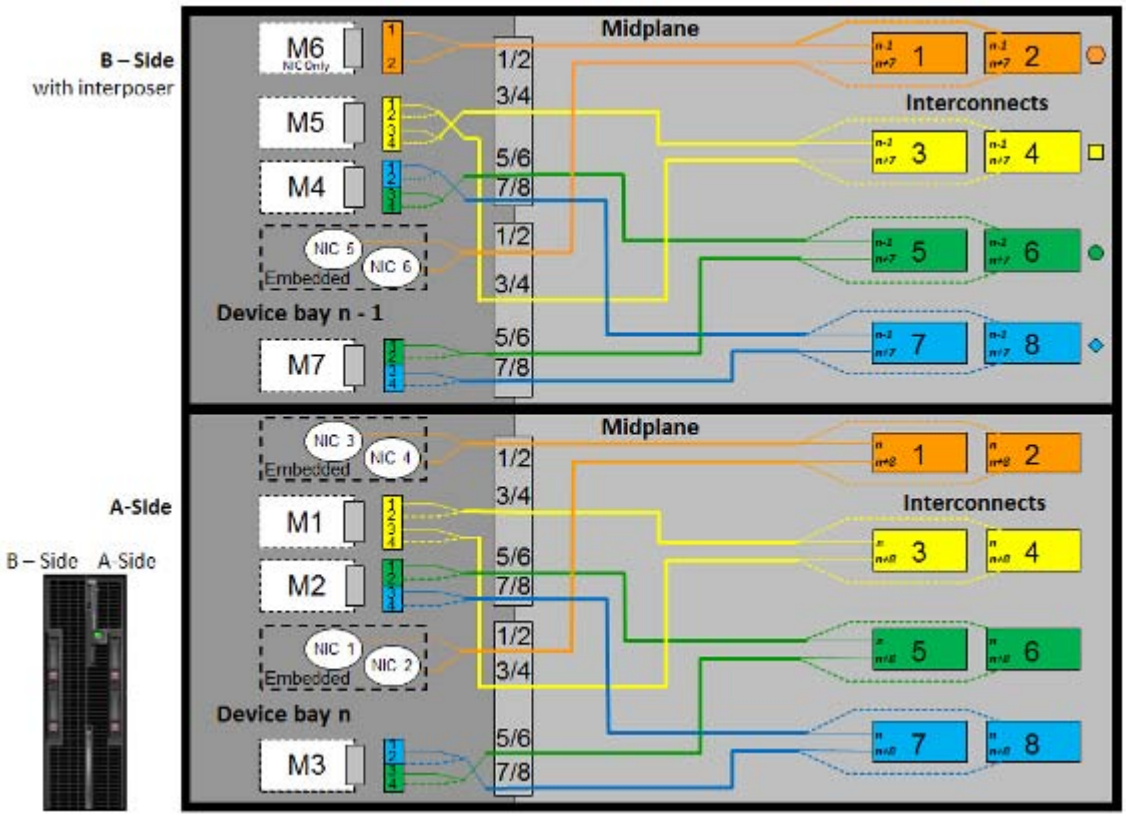
Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c (G1)–G6



Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c G7



Server Blades voller Höhe und doppelter Breite wie z. B. HP ProLiant BL680c G7



Tabellenansicht der Portzuordnungen der Geräteeinschübe für das c7000-Gehäuse

Die Server Blades werden den Verbindungsmoduleinschüben folgendermaßen zugeordnet. Die Begriffe „1x“, „2x“ oder „4x“ beziehen sich auf die Anzahl von Verbindungsleitungen pro Port, die vom Controller bereitgestellt werden. Wenn ein Gerät nicht vorhanden ist, ist das Kontrollkästchen deaktiviert und der Port kann nicht angezeigt werden.

- Beispiele für 1x-Ports sind 1 GB Ethernet (1 GbE), 10 GB Ethernet (10 GbE) und alle Fibre Channel-Geräte.
- Beispiele für 2x-Ports sind 20 GB Ethernet (20 GbE) und alle seriell angeschlossenen SCSI (SAS)-Geräte.
- Beispiele für 4x-Ports sind alle InfiniBand-Geräte.
- In den folgenden Tabellen werden die Ethernet-Ports als NICs bezeichnet.

Server Blades halber Höhe und einfacher Breite

Die folgende Tabelle führt die Portzuordnung für die in einem c7000-Geräteeinschub N (1–16) halber Höhe installierten Server Blades halber Höhe auf. Beispiele für solche Server Blades halber Höhe sind HP ProLiant BL260c, BL280c, BL420c, BL465c, BL490c, BL495c und WS460c.

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
NIC[1]	NIC 1	1/Port N	Ein oder zwei Ethernet-Verbindungsmodule mit einfacher Breite
	NIC 2	2/Port N	

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
Mezzanine-Steckplatz 1: 1x- oder 2x-Karten	1x-/2x-Port 1 1x-/2x-Port 2	3/Port N 4/Port N	• Ein Verbindungsmodul einfacher Breite • Vier Port-Karten, wobei nur eine Verbindung zu den ersten beiden Ports hergestellt wird.
Mezzanine-Steckplatz 1: 4x-Karten	4x-Port 1	3/Port N	• Ein Verbindungsmodul doppelter Breite • Es wird nur eine Verbindung zu Port 1 einer Zwei-Port-Karte hergestellt.
Mezzanine-Steckplatz 2: 1x- oder 2x-Karten	1x-/2x-Port 1 1x-/2x-Port 2 1x-/2x-Port 3 1x-/2x-Port 4	5/Port N 6/Port N 7/Port N[2] 8/Port N[2]	Ein oder zwei Verbindungsmodule einfacher Breite
Mezzanine-Steckplatz 2: 4x-Karten	4x-Port 1 4x-Port 2	5/Port N 7/Port N[2]	Ein oder zwei Verbindungsmodule mit doppelter Breite

[1] G7 und frühere Generationen von Server Blades verfügen über auf der Systemplatine integrierte Ethernet-Ports. Bei Server Blades ab Gen8 befinden sich die Ethernet-Ports auf einer vom Benutzer auswählbaren Karte, die als FlexibleLOM-Adapter bezeichnet wird. Für die Ports des FlexibleLOM-Adapters und für die integrierten Netzwerkadapter-Ports gilt die gleiche Zuordnung.
[2] Ein Anschluss an Verbindungsmoduleinschübe 7 und 8 ist nur mit Mezzanine Cards mit 4 Ports oder Port 2 der 4x-Karte in Mezzanine-Steckplatz 2 möglich.

Server Blades voller Höhe und einfacher Breite

Die folgende Tabelle listet die Portzuordnung der in einem c3000-Geräteeinschub N (1-4) voller Höhe installierten Server Blades voller Höhe und einfacher Breite auf. Beispiele für solche Server Blades voller Höhe sind HP ProLiant BL680c (G1), BL680c Gen5 und BL480c, BL620c, BL660c und BL685c.

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
NIC[1]	NIC 1 NIC 2 NIC 3 NIC 4	1/Port N+8 2/Port N+8 1/Port N 2/Port N	Ein oder zwei Ethernet-Verbindungsmodule mit einfacher Breite
Mezzanine-Steckplatz 1: 1x- oder 2x-Karten	1x-/2x-Port 1 1x-/2x-Port 2 1x-/2x-Port 3 1x-/2x-Port 4	3/Port N 4/Port N 3/Port N+8 4/Port N+8	Eine oder zwei Verbindungsmodule einfacher Breite
Mezzanine-Steckplatz 1: 4x-Karten	4x-Port 1	3/Port N	• Ein Verbindungsmodul doppelter Breite

Verbindung	Portnummer	Anschluss an Verbindungsmodul-einschub/Port	Anmerkungen
			• Bei einer Karte mit 2 Ports kann nur eine Verbindung zu Port 1 hergestellt werden.
Mezzanine-Steckplatz 2: 1x- oder 2x-Karten	1x-/2x-Port 1	5/Port N	Bis zu vier Verbindungsmodule mit einfacher Breite
	1x-/2x-Port 2	6/Port N	
	1x-/2x-Port 3	7/Port N[2]	
	1x-/2x-Port 4	8/Port N[2]	
Mezzanine-Steckplatz 2: 4x-Karten	4x-Port 1	5/Port N	Ein oder zwei Verbindungsmodule mit doppelter Breite
	4x-Port 2	7/Port N[2]	
Mezzanine-Steckplatz 3: 1x- oder 2x-Karten	1x-/2x-Port 1	7/Port N+8*	Bis zu vier Verbindungsmodule mit einfacher Breite
	1x-/2x-Port 2	8/Port N+8*	
	1x-/2x-Port 3	5/Port N[2]	
	1x-/2x-Port 4	6/Port N[2]	
Mezzanine-Steckplatz 3: 4x-Karten	4x-Port 1	5/Port N+8	Ein oder zwei Verbindungsmodule mit doppelter Breite
	4x-Port 2	7/Port N+8*	

[1] G7 und frühere Generationen von Server Blades verfügen über auf der Systemplatine integrierte Ethernet-Ports. Bei Server Blades ab Gen8 befinden sich die Ethernet-Ports auf einer vom Benutzer auswählbaren Karte, die als FlexibleLOM-Adapter bezeichnet wird. Für die Ports des FlexibleLOM-Adapters und für die integrierten Netzwerkadapter-Ports gilt die gleiche Zuordnung.
[2] Ein Anschluss an Verbindungsmoduleinschübe 7 und 8 ist nur mit Mezzanine Cards mit 4 Ports oder Port 2 der 4x-Karte in Mezzanine-Steckplatz 2 möglich.

Server Blades halber Höhe und doppelter Dichte

In der folgenden Tabelle werden die verfügbaren Konfigurationen für die in einem c7000-Geräteeinschub N (1–16) halber Höhe installierten Server Blades doppelter Dichte aufgeführt. Beispiele für solche Server Blades doppelter Dichte sind HP ProLiant BL2x220c (G1) – G6.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC von Server A	NIC 1 (Port:1)	1/Port N
	NIC 2 (Port:2)	3/Port N
Mezzanine von Server A*	Port 1	5/Port N
	Port 2	6/Port N
Integrierter NIC von Server B	NIC 1 (Port:1)	2/Port
	NIC 2 (Port:2)	4/Port N
Mezzanin von Server B*	Port 1	7/Port N
	Port 2	8/Port N

Server Blades halber Höhe und doppelter Dichte wie z. B. HP ProLiant BL2x220c G7

In der folgenden Tabelle werden die verfügbaren Konfigurationen für in einem c7000-Geräteeinschub N (1–16) halber Höhe installierte Server Blades doppelter Dichte, wie z. B. ProLiant BL2x220c G7, aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC von Server A	NIC 1 (Port:1)	1/Port N
	NIC 2 (Port:2)	3/Port N
Server A NC543i*	Port 1	5/Port N
Integrierter NIC von Server B	NIC 1 (Port:1)	2/Port N
	NIC 2 (Port:2)	4/Port N
Server B NC543i*	Port 1	7/Port N

***** Der im HP ProLiant BL2x220c G7 Server Blade integrierte NC543i wird automatisch von Onboard Administrator für Ethernet konfiguriert, wenn in Einschub 3 ein Ethernet-Verbindungsmodul installiert ist, oder für InfiniBand, wenn in Einschub 3 ein InfiniBand-Verbindungsmodul doppelter Breite installiert ist. Um die NC543i-Konfiguration zum jeweils anderen Typ zu ändern, schalten Sie alle HP ProLiant BL2x220c G7 Server Blades aus, und ersetzen Sie das Verbindungsmodul durch den jeweils anderen Typ. Wenn Sie das aktive Onboard Administrator-Modul neu starten oder alle HP ProLiant BL2x220c G7 Server Blades erneut einstecken, dann konfiguriert der Onboard Administrator alle integrierten NC543i-Geräte entsprechend des neuen Verbindungstyps neu.

AMC Telco I/O-Erweiterungs-Blade

In der folgenden Tabelle werden die verfügbaren Konfigurationen für die in einem c7000-Geräteeinschub N (1–16) installierten AMC Telco-Geräte aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
AMC integriert (1)	Port 1	1/Port N
	Port 2	2/Port N
	Port 3	3/Port N
	Port 4	4/Port N
AMC integriert (2)	Port 5	5/Port N
	Port 6	6/Port N
	Port 7	7/Port N
	Port 8	8/Port N

Server Blades voller Höhe und doppelter Breite wie z. B. HP ProLiant BL680c G7

In der folgenden Tabelle wird die Portzuordnung für die in einem c7000-Geräteinschub N (2, 4, 6 oder 8) voller Höhe installierten Server Blades voller Höhe und doppelter Breite, wie z. B. HP ProLiant BL680c G7, aufgeführt.

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC auf Seite A	NIC 1	1/Port N+8
	NIC 2	2/Port N+8
	NIC 3	1/Port N
	NIC 4	2/Port N

Verbindung	Portnummer	Anschluss an Verbindungsmodul- einschub/Port
Integrierter NIC auf Seite B	NIC 5	1/Port N+7
	NIC 6	2/Port N+7
Mezzanine 1 auf Seite A	Port 1	3/Port N
	Port 2	4/Port N
	Port 3	3/Port N+8
	Port 4	4/Port N+8
Mezzanine 2 auf Seite A	Port 1	5/Port N
	Port 2	6/Port N
	Port 3	7/Port N
	Port 4	8/Port N
Mezzanine 3 auf Seite A	Port 1	7/Port N+8
	Port 2	8/Port N+8
	Port 3	5/Port N+8
	Port 4	6/Port N+8
Mezzanine 4 auf Seite B	Port 1	7/Port N-1
	Port 2	8/Port N-1
	Port 3	5/Port N-1
	Port 4	6/Port N-1
Mezzanine 5 auf Seite B	Port 1	3/Port N+7
	Port 2	4/Port N+7
	Port 3	3/Port N-1
	Port 4	4/Port N-1
Mezzanine 6 auf Seite B	Port 1	1/Port N-1
Nur NIC	Port 2	2/Port N-1
Mezzanine 7 auf Seite B	Port 1	5/Port N+7
	Port 2	6/Port N+7
	Port 3	7/Port N+7
	Port 4	8/Port N+7

Firmware

Um Firmwareinformationen zu den Geräteeinschubs-Komponenten anzuzeigen und eine manuelle Ermittlung und manuelle Aktualisierung der Firmware durchzuführen, klicken Sie auf **Firmware**. Weitere Informationen zu Support-Anforderungen und Leistungsproblemen finden Sie unter „Gehäuse-Firmwareverwaltung“ (Enclosure Firmware Management auf Seite 197).

Firmware-Übersichtsinformationen

Zeile	Beschreibung
Bay (Einschub)	Der Geräteeinschub innerhalb des Gehäuses.
Device Model (Komponentenmodell)	Die Modellnummer der Komponente.
Firmware Component (Firmwarekomponente)	Die Komponente, für die die Firmware-Informationen bereitgestellt werden.
Current Version (Aktuelle Version)	Die Version der auf der Komponente installierten Firmware.
Firmware ISO Version (Firmware-ISO-Version)	Die neueste Version der Firmware, die zur Installation auf der Komponente verfügbar ist.

HINWEIS: Wenn die Blade-Firmware nach der Ermittlung und Aktualisierung eines Servers nicht mit der DVD-ISO-Firmware übereinstimmt, wird ein Informationssymbol angezeigt.

HINWEIS: Ein Buchstabe nach der Firmwareversion bedeutet, dass die Versionshinweise für eine intelligente Komponente überarbeitet wurden. Diese Überarbeitung ist keine funktionelle Firmwareaktualisierung.

Manuelle Ermittlung

Eine manuelle Ermittlung führt einen Start zur Ermittlung auf dem Server durch, sammelt erweiterte Firmware-Informationen für diesen Server und startet den Server neu zum normalen Betrieb.

Um den Ermittlungsvorgang auf dem ausgewählten Server zu starten, klicken Sie auf **Start Manual Discovery** (Manuelle Ermittlung starten).

Wenn auf dem Server Blade „Secure Boot“ (Sicherer Systemstart) konfiguriert ist, kann keine manuelle Ermittlung durchgeführt werden. Die Schaltfläche **Start Manual Discovery** (Manuelle Ermittlung starten) wird abgeblendet. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich den Administrator) am Durchführen dieses Vorgangs über das Server Blade-Betriebssystem oder iLO. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Manuelle Aktualisierung

Eine manuelle Aktualisierung führt einen Start zur Aktualisierung auf dem Server durch, aktualisiert die Firmware für diesen Server und startet anschließend den Server neu zum normalen Betrieb.

Um den Aktualisierungsvorgang auf den ausgewählten Servern zu starten, klicken Sie auf **Start Manual Update** (Manuelle Aktualisierung starten).

Wenn auf dem Server Blade „Secure Boot“ (Sicherer Systemstart) konfiguriert ist, kann keine manuelle Aktualisierung durchgeführt werden. Die Schaltfläche **Start Manual Update** (Manuelle Aktualisierung starten) wird abgeblendet. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich den Administrator) am Durchführen dieses Vorgangs über das Server Blade-Betriebssystem oder iLO. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Weitere Informationen zur manuellen Ermittlung und manuellen Aktualisierung finden Sie unter „Starten einer manuellen Aktualisierung oder Ermittlung“ (Starten einer manuellen Aktualisierung oder Ermittlung auf Seite 272).

Firmware-Protokoll

Dieses Protokoll zeigt detaillierte Informationen zu dem zuletzt auf dem Server ausgeführten Enclosure Firmware Management-Vorgang an. Dieses Protokoll ist serverspezifisch und wird immer

dann gelöscht, wenn auf dem Server ein neuer Enclosure Firmware Management-Vorgang gestartet wird. Dieses Protokoll wird auch dann gelöscht, wenn der Server aus dem Gehäuse entfernt wird, sowie im Modus „Set Factory“ (Werkseinstellungen festlegen).

Das Firmware-Protokoll ist die nützlichste Ressource zum Bestimmen des Status eines Enclosure Firmware Management-Vorgangs auf einem bestimmten Server.

Weitere Informationen zum Firmwareprotokoll finden Sie unter „Protokollieren“ (Firmware-Management-Protokolle auf Seite 275).

Sitzungsprotokoll

Dieses Protokoll zeigt detaillierte Informationen zu dem zuletzt auf dem Server ausgeführten Enclosure Firmware Management-Vorgang an und protokolliert die gesamte Sitzung im iLO VSP. Dieses Protokoll ist serverspezifisch und wird immer dann gelöscht, wenn auf dem Server ein neuer Enclosure Firmware Management-Vorgang gestartet wird. Dieses Protokoll wird auch dann gelöscht, wenn der Server aus dem Gehäuse entfernt wird.

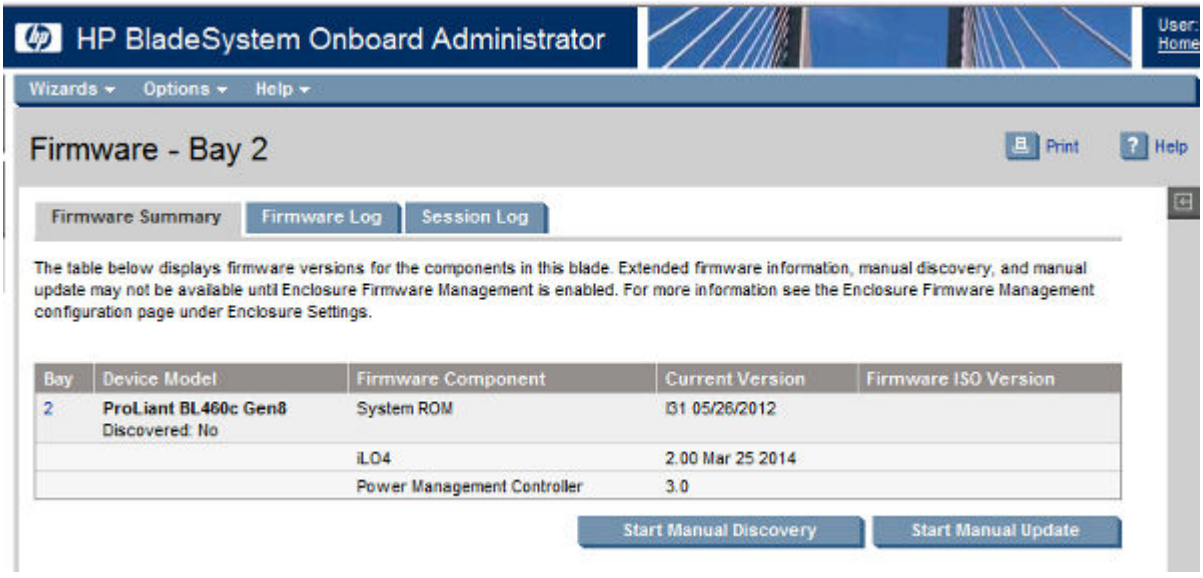
Weitere Informationen zum Sitzungsprotokoll finden Sie unter „Protokollieren“ (Firmware-Management-Protokolle auf Seite 275).

Starten einer manuellen Aktualisierung oder Ermittlung

HINWEIS: Der Onboard Administrator darf nicht durch Flashen aktualisiert oder neu starten, während eine Enclosure Firmware Management-Aufgabe ausgeführt wird.

HINWEIS: Wenn auf dem Server Blade „Secure Boot“ (Sicherer Systemstart) konfiguriert ist, kann keine manuelle Ermittlung oder manuelle Aktualisierung durchgeführt werden. Die Schaltflächen **Start Manual Discovery** (Manuelle Ermittlung starten) und **Start Manual Update** (Manuelle Aktualisierung starten) sind abgeblendet. „Secure Boot“ (Sicherer Systemstart) hindert Benutzer (einschließlich den Administrator) am Durchführen dieser Vorgänge über das Server Blade-Betriebssystem oder iLO. Startvorgänge können nur über das im BIOS vom Administrator konfigurierte Startgerät durchgeführt werden.

Einzelne Server



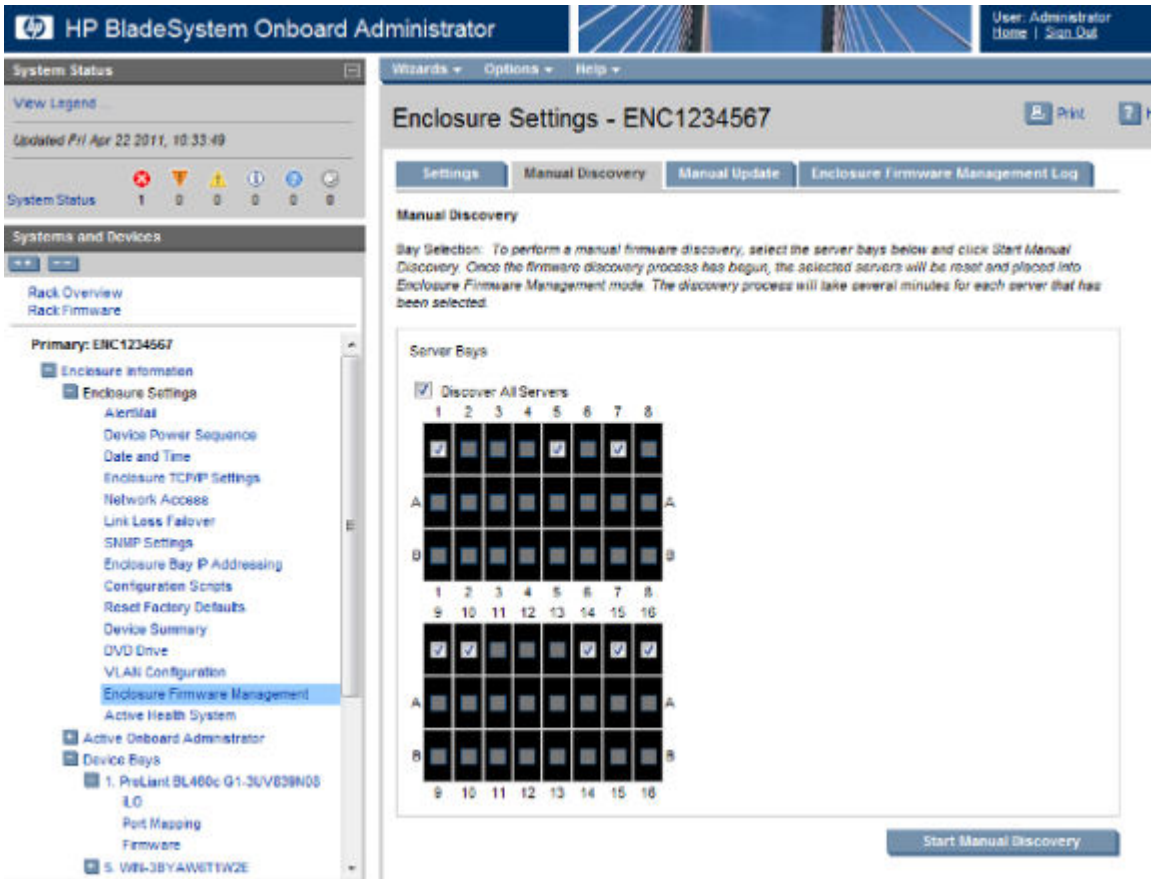
So starten Sie eine manuelle Aktualisierung oder Ermittlung auf einzelnen Servern:

1. Wählen Sie in der linken Strukturansicht **Device Bays** (Geräteeinschübe) aus. Wählen Sie den gewünschten anzuzeigenden Einschub und anschließend **Firmware** aus.
2. Klicken Sie auf **Start Manual Discovery** (Manuelle Ermittlung starten) oder **Start Manual Update** (Manuelle Aktualisierung starten).

Mehrere Server

So starten Sie eine manuelle Ermittlung auf mehreren Servern:

1. Wählen Sie in der linken Strukturansicht **Enclosure Settings (Gehäuseeinstellungen)>Enclosure Firmware Management**.
2. Wählen Sie die Registerkarte **Manual Discovery** (Manuelle Ermittlung) aus.

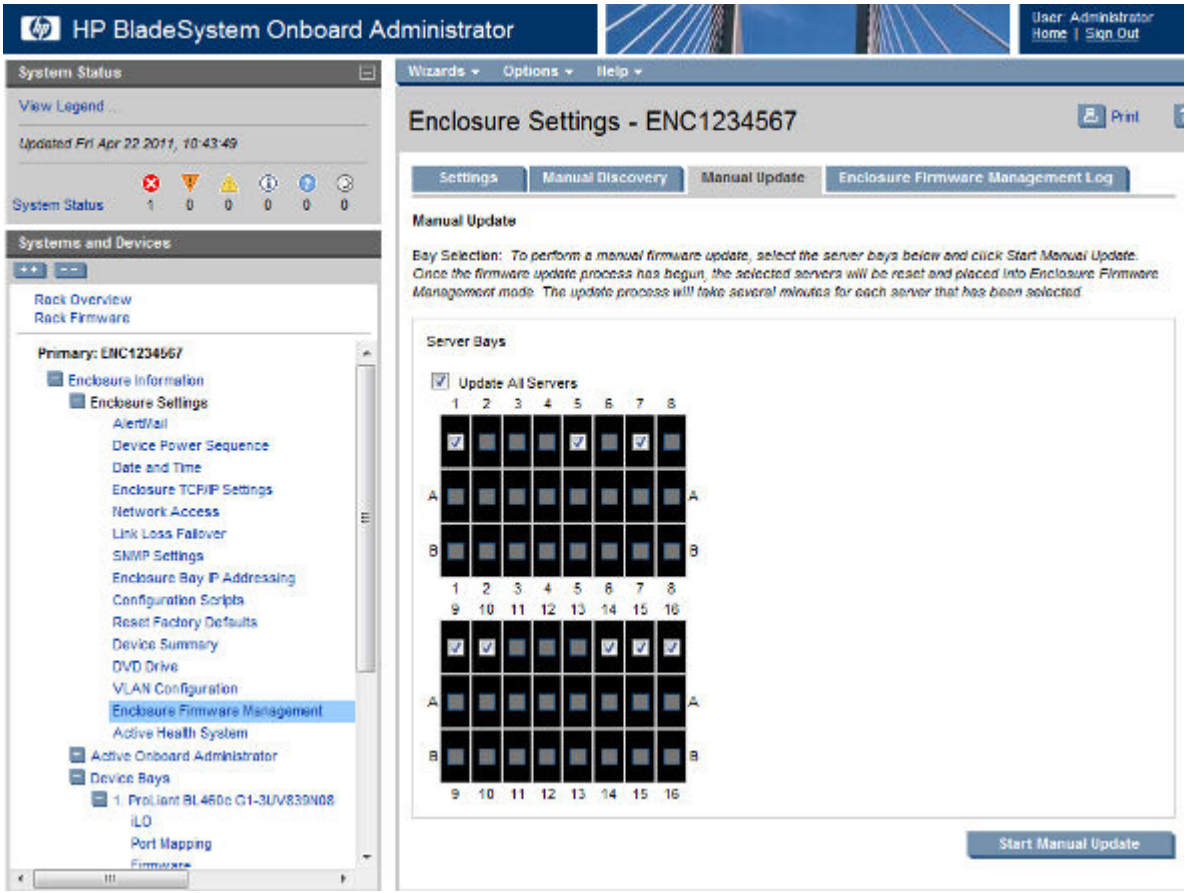


3. Aktivieren Sie das Kontrollkästchen neben den betreffenden Servereinschüben oder aktivieren Sie das Kontrollkästchen **Discover All Servers** (Alle Server ermitteln).
4. Klicken Sie auf **Start Manual Discovery** (Manuelle Ermittlung starten).

So starten Sie eine manuelle Aktualisierung auf mehreren Servern:

1. Wählen Sie in der linken Strukturansicht **Enclosure Settings (Gehäuseeinstellungen)>Enclosure Firmware Management**.

2. Wählen Sie die Registerkarte **Manual Update** (Manuelle Aktualisierung) aus.

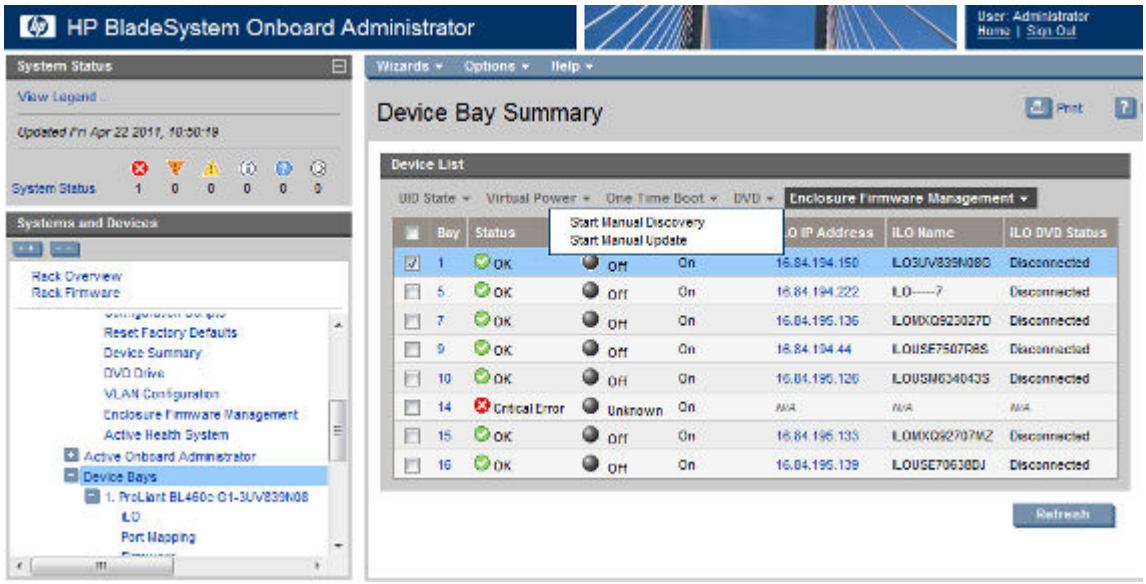


3. Aktivieren Sie das Kontrollkästchen neben den betreffenden Servereinschüben oder aktivieren Sie das Kontrollkästchen **Update All Servers** (Alle Server aktualisieren).
4. Klicken Sie auf **Start Manual Update** (Manuelle Aktualisierung starten).

So starten Sie eine manuelle Ermittlung oder Aktualisierung über den Bildschirm „Device Bays“ (Geräteeinschübe):

1. Wählen Sie in der linken Strukturansicht **Device Bays** (Geräteeinschübe) aus.
2. Aktivieren Sie das Kontrollkästchen neben dem betreffenden Einschub.

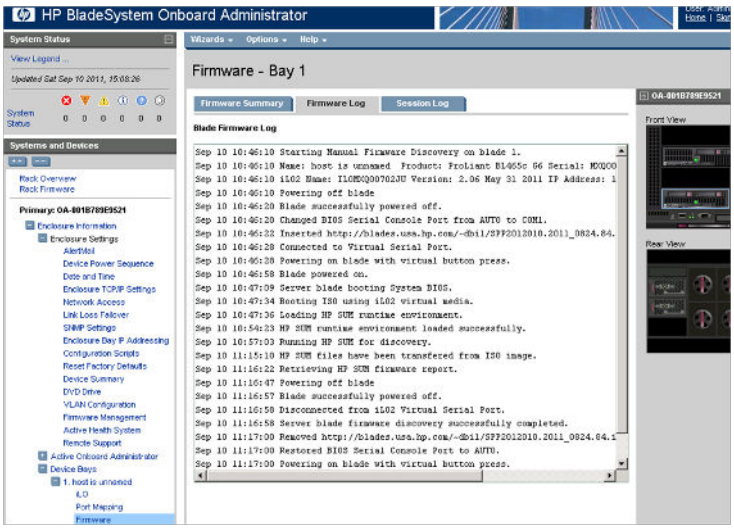
3. Wählen Sie im Menü „Firmware Management“ **Start Manual Discovery** (Manuelle Ermittlung starten) oder **Start Manual Update** (Manuelle Aktualisierung starten) aus.



Firmware-Management-Protokolle

Enclosure Firmware Management-Ereignisse werden in drei Protokolle geschrieben. Die folgenden Abschnitte beschreiben den Typ der in jedes Protokoll aufgenommenen Ereignisse. Alle Protokolle können zur Überprüfung des Status und für abschließende Aufgaben sowie für Fehlerbeseitigungszwecke verwendet werden.

Firmware-Protokoll

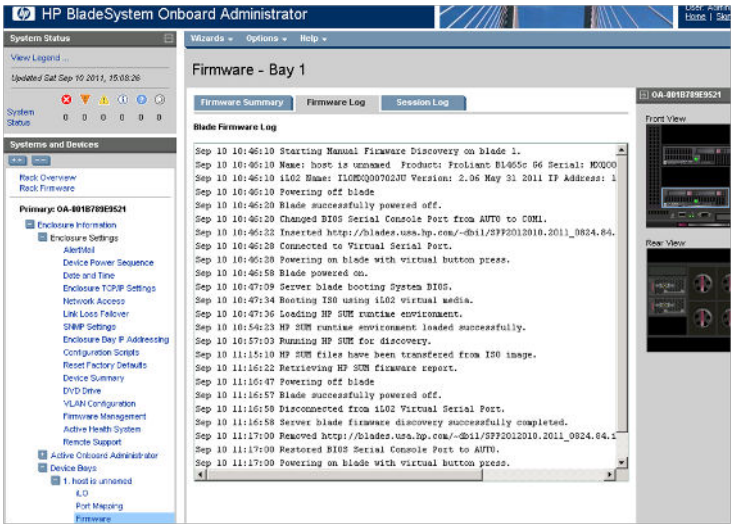


Dieses Protokoll zeigt detaillierte Informationen zu dem zuletzt auf dem Server ausgeführten Enclosure Firmware Management-Vorgang an. Dieses Protokoll ist serverspezifisch und wird immer dann gelöscht, wenn auf dem Server ein neuer Enclosure Firmware Management-Vorgang gestartet wird. Dieses Protokoll wird auch dann gelöscht, wenn der Server aus dem Gehäuse entfernt wird, sowie im Modus „Set Factory“ (Werkseinstellungen festlegen).

Dieses Protokoll ist über OA-Neustarts und Stromausfälle hinweg beständig. Es wird auf dem Standby-OA beibehalten, falls vorhanden.

Das Firmware-Protokoll ist die nützlichste Ressource zum Bestimmen des Status eines Enclosure Firmware Management-Vorgangs auf einem bestimmten Server.

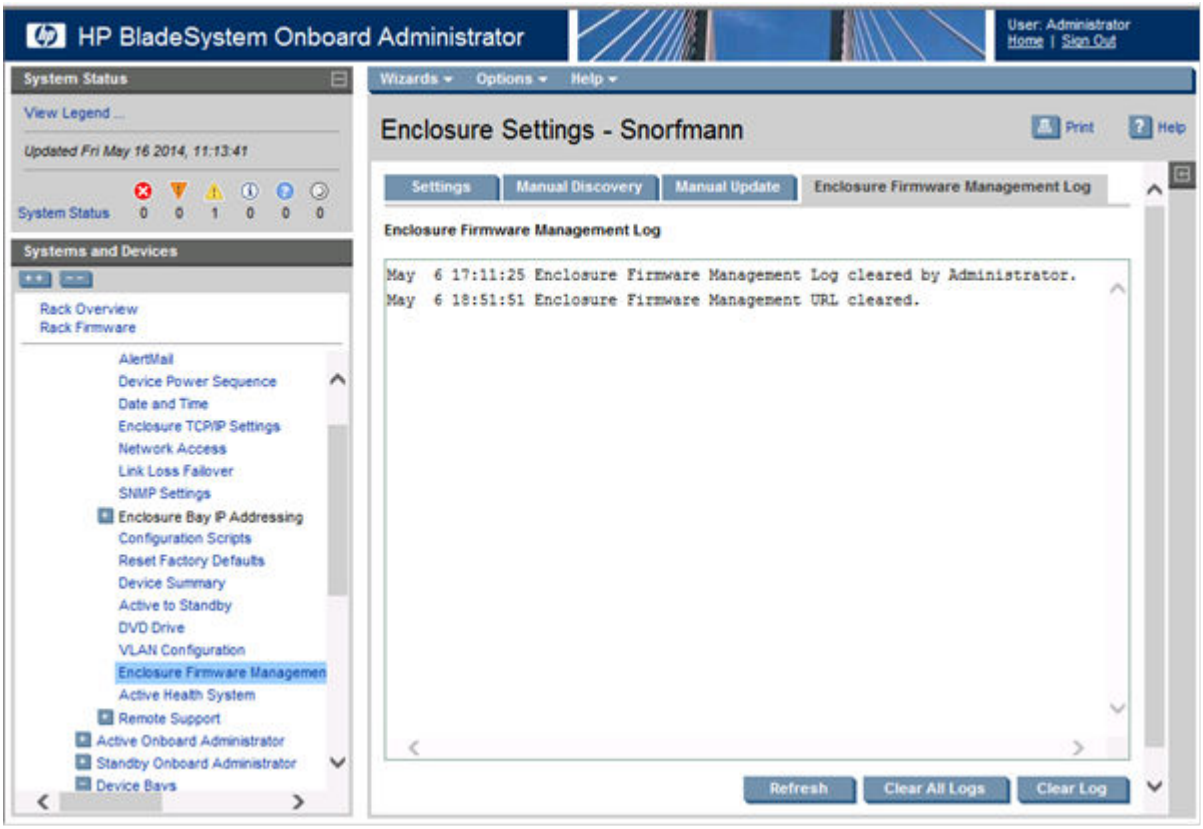
Sitzungsprotokoll



Dieses Protokoll zeigt detaillierte Informationen zu dem zuletzt auf dem Server ausgeführten Enclosure Firmware Management-Vorgang an und protokolliert die gesamte Sitzung im iLO VSP. Dieses Protokoll ist serverspezifisch und wird immer dann gelöscht, wenn auf dem Server ein neuer Enclosure Firmware Management-Vorgang gestartet wird. Dieses Protokoll wird auch dann gelöscht, wenn der Server aus dem Gehäuse entfernt wird.

Dieses Protokoll ist über OA-Neustarts und Stromausfälle hinweg beständig. Es wird auf dem Standby-OA beibehalten, falls vorhanden.

Enclosure Firmware Management-Protokoll



Das Enclosure Firmware Management-Protokoll bietet eine konsolidierte Ansicht der wichtigsten Enclosure Firmware Management-Ereignisse, wie z. B. Firmware-Image-Auswahl, Richtlinien- und Zeitplanänderungen sowie gestartete und abgeschlossene Firmware-Vorgänge. Dieses Protokoll enthält nicht die schrittweisen Details, die im Firmware-Protokoll eines jeden Servers enthalten sind.

Das Enclosure Firmware Management-Protokoll ist über OA-Neustarts und Stromausfälle hinweg beständig. Es wird auf dem Standby-OA beibehalten, falls vorhanden.

Um aktualisierte Protokollinformationen anzuzeigen, klicken Sie auf **Refresh** (Aktualisieren).

Um Informationen für das Enclosure Firmware Management-Protokoll und das serverspezifische Firmware- und Sitzungsprotokoll zu löschen, klicken Sie auf **Clear All Logs** (Alle Protokolle löschen).

Um Informationen für das Enclosure Firmware Management-Protokoll zu löschen, klicken Sie auf **Clear Log** (Protokoll löschen).

⚠ **ACHTUNG:** Einmal gelöschte Daten können nicht wiederhergestellt werden.

Informationen über die fehlgeschlagene Ereignisse finden Sie unter „Enclosure Firmware Management-Protokoll“ (Enclosure Firmware Management-Protokoll auf Seite 205).

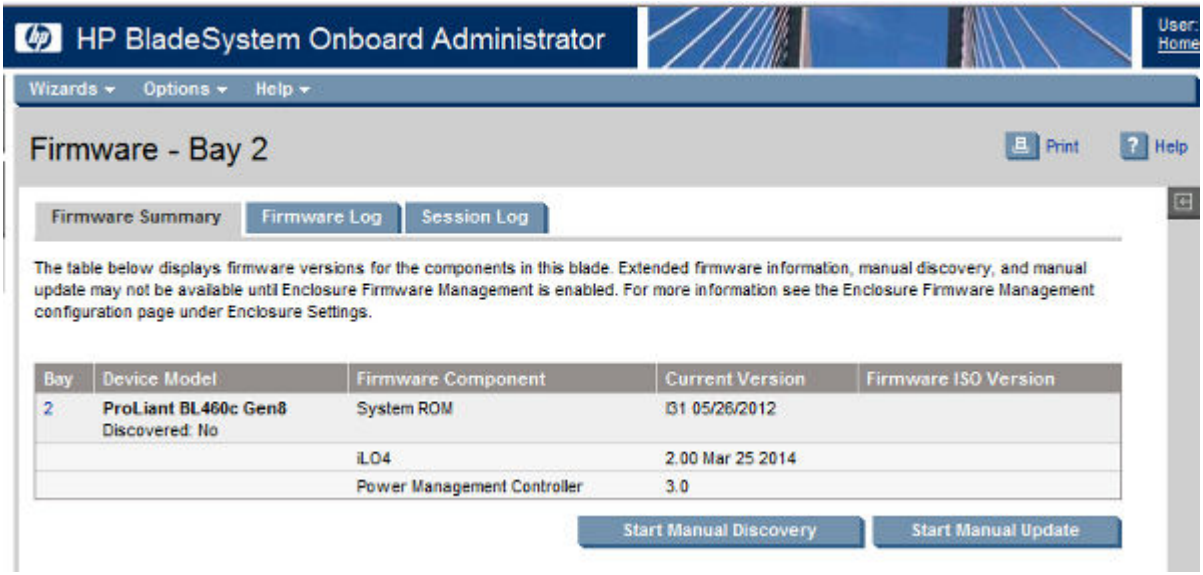
Anzeigen der Firmware-Versionen

Nachdem eine Enclosure Firmware Management-Aufgabe erfolgreich durchgeführt wurde, überprüfen Sie, ob die Firmwareversionen aller zum Aktualisieren ausgewählten Geräte aktualisiert wurden. Ein erfolgreicher Abschluss einer Enclosure Firmware Management-Aufgabe bedeutet möglicherweise nicht, dass die Firmware auf die Versionen auf dem ISO-Image aktualisiert wurde. Weitere Informationen finden Sie unter „Abweichende Firmwareversionen“ (Abweichende Firmwareversionen auf Seite 279).

Server-Firmware

Wählen Sie in der linken Strukturansicht **Device Bays** (Geräteeinschübe) aus. Wählen Sie den Einschub, der angezeigt werden soll, und klicken Sie dann auf **Firmware**.

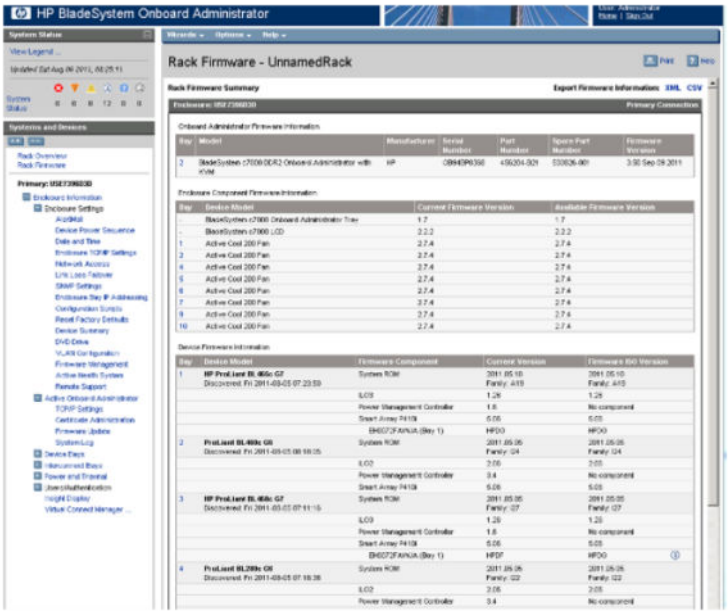
Die erweiterten Server-Firmware-Informationen erscheinen auf der Onboard Administrator-GUI oder -CLI eines jeden Servers. Ein Firmware-Management-Protokoll für jeden Server Blade zeigt eine Aufzeichnung der Schritte während des letzten Firmwareaktualisierungs- oder Ermittlungsereignisses an. Die Firmware-Übersicht zeigt Datum und Uhrzeit an, an dem die letzte Ermittlung oder Aktualisierung stattfand. Wenn der Server Blade aus dem Gehäuse entfernt wird, dann wird dieses Protokoll gelöscht. Diese Protokolle werden mit dem Onboard Administrator-Standby-Modul synchronisiert, sofern vorhanden. Die Protokolle werden im Flash-Speicher gespeichert, so dass die Informationen nach einem Neustart des Onboard Administrators weiterhin verfügbar sind.



Rack-Firmware

Wählen Sie oben in der linken Strukturansicht **Rack Firmware** (Rack-Firmware) aus.

Die Onboard Administrator-GUI oder -CLI stellt einen Bericht des aktuellen Firmwarebestands in jedem Gehäuse bereit. Bei miteinander verbundenen Gehäusen zeigt die GUI die Firmware über alle verknüpften Gehäuse hinweg an. Der Bericht umfasst die aktuelle Firmwareversion von Server-BIOS, iLO, PMC, NIC, FC HBA, Smart Array und eines jeden installierten, am Smart Array angeschlossenen Festplattenlaufwerks. Diese Informationen erleichtert die Diagnose komplexer Netzwerk- oder FC-SAN-Probleme, die durch inkorrekte NIC- oder FC-HBA-Firmwareversionen verursacht werden.



Abweichende Firmwareversionen

Die folgenden Szenarien können dazu führen, dass irreguläre Firmwareversions- oder Statusinformationen erscheinen:

- Ein Buchstabe nach der Firmwareversion bedeutet, dass die Versionshinweise für eine intelligente Komponente überarbeitet wurden. Diese Überarbeitung ist keine funktionelle Firmwareaktualisierung.
- Wenn als Firmware-ISO-Version `No Component` (Keine Komponente) angezeigt wird, bedeutet dies, dass das SPP-Image keine Firmware für diese Komponente enthält. Dieses Szenario tritt gewöhnlich bei dem Power Management Controller in ProLiant G7 Servern ein.
- Wenn das informative Symbol erscheint, stimmt die Firmware des Server Blade nach der Ermittlung oder Aktualisierung eines Servers nicht mit der DVD-ISO-Firmware überein.
- Wenn bei NIC, FC HBA, Smart Array oder installierten, am Smart Array angeschlossenen Festplattenlaufwerken eine Flash-Aktualisierung ohne das Enclosure Firmware Management-Utility vorgenommen wird, kann der Onboard Administrator diese Informationen nicht auslegen und meldet weiterhin Firmware-Informationen basierend auf dem letzten Enclosure Firmware Management-Vorgang.
- Wenn Firmware mit dem Enclosure Firmware Management-Dienstprogramm nicht aktualisiert wird, spiegelt die mit dem Dienstprogramm vorgenommene Überwachung und Berichterstellung keine mit anderen Tools vorgenommenen Änderungen wider.

  Die EFM-Überwachung und -Berichterstellung tragen nicht den mit anderen Tools, wie z. B. HP SUM und HP SIM, vorgenommenen Änderungen Rechnung, wenn die Firmware auf einem Blade nicht mittels EFM aktualisiert wurde. Korrekte Versionen der Firmware werden gemeldet, sobald die EFM-Ermittlung oder -Aktualisierung durchgeführt wurde.

Speicher-Blades

Im Menü **Systems and Devices** (Systeme und Komponenten) werden in der Kategorie „Device Bays“ (Geräteeinschübe) alle Server Blades und Speicher-Blades aufgelistet. Bei Auswahl der Menüoption für ein Speicher-Blade wird die Statusseite des jeweiligen Speicher-Blade angezeigt (bei Klicken auf das Symbol **+** links neben der Menüoption wird die Speicher-Blade-Ansicht nicht erweitert). Es sind

drei Registerkarten verfügbar, die spezifische Informationen zum Speicher-Blade anzeigen: **Status**, **Information** (Informationen) und **Virtual Devices** (Virtuelle Geräte).

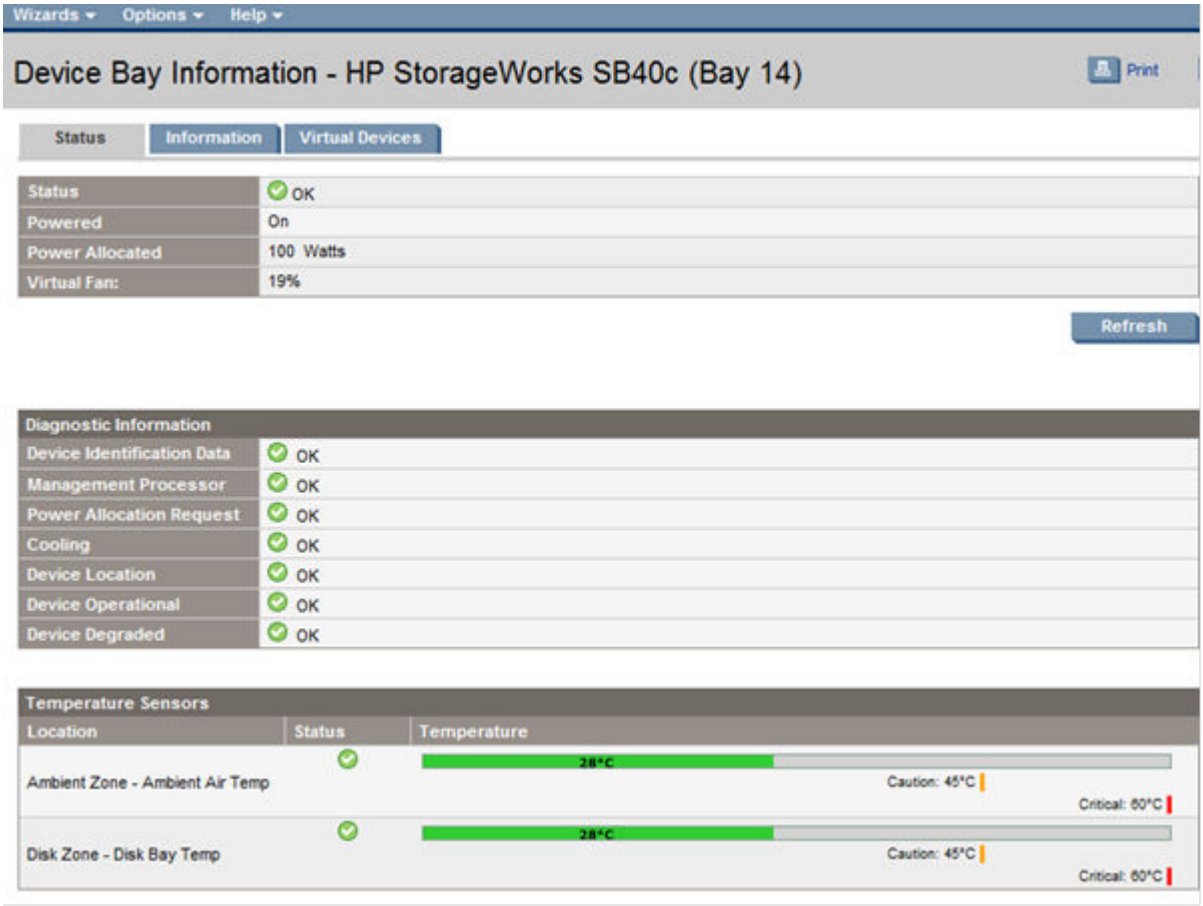
Speicher-Blades werden direkt neben Server Blades in das Gehäuse eingesetzt, wobei physische Platzierungsregeln zu beachten sind. Auch muss sichergestellt werden, dass der Speicher-Blade nicht eingeschaltet wird, bevor der Server Blade eingeschaltet und mit ihm gepaart wird.

Bei Einsatz von Server Blades mit halber Bauhöhe muss der Speicher-Blade in den links vom Server Blade liegenden Gehäusesteckplatz eingesteckt werden. Für jeden im Gehäuse installierten Server Blade kann links davon ein zugehöriger Speicher-Blade in das Gehäuse eingesetzt werden (maximal sind acht Server Blades und acht Speicher-Blades zulässig).

Bei Einsatz von Server Blades mit voller Bauhöhe muss der Speicher-Blade in den links vom Server Blade liegenden unteren Gehäusesteckplatz eingesteckt werden. Wird der Speicher-Blade im oberen linken Steckplatz des Gehäuse platziert, kann dies bei der mit ihm gepaarten Komponenten einen Fehler auslösen. Es kann sich ein Server Blade mit halber Bauhöhe in dem Steckplatz links oben neben einem Server Blade mit voller Bauhöhe befinden, während sich links unten neben dem Server Blade voller Bauhöhe ein Speicher-Blade befindet.

Server Blades voller Bauhöhe benötigen zur Kommunikation mit dem entsprechenden Speicher-Blade eine Mezzanine Card. Wenn ein Speicher-Blade ordnungsgemäß neben einem Server Blade voller Höhe platziert wird, im Server Blade jedoch keine passende Mezzanine Card vorhanden ist, tritt selbst dann ein Konfigurationsfehler, jedoch kein „Partner Device Error“ (Komponentenpaarungsfehler) auf, wenn der Speicher-Blade korrekt neben dem Server Blade voller Bauhöhe platziert ist.

Wird die Stromzufuhr zu einem Server Blade unterbrochen, wird auch der zugehörige Speicher-Blade nicht mit Strom versorgt.



Zeile	Beschreibung
Status (Zustand)	Der allgemeine Status des Speicher-Blades. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Powered (Netzbetrieb)	Der Stromversorgungszustand des Speicher-Blades. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
Power Allocated (Zugewiesene Stromversorgung)	Die Menge der dem Speicher-Blade zum Verbrauch zugewiesenen Stromversorgung in Watt.
Virtual Fan (Virtueller Lüfter)	Maximale Umdrehungen pro Minute (RPM) des virtuellen Lüfters in Prozent.
Partner Device* (Gepaarte Komponente*)	Zeigt an, mit welchem Server Blade und Einschub der Speicher-Blade verknüpft ist.

* Nicht abgebildet

Diagnostic information (Diagnoseinformationen)

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

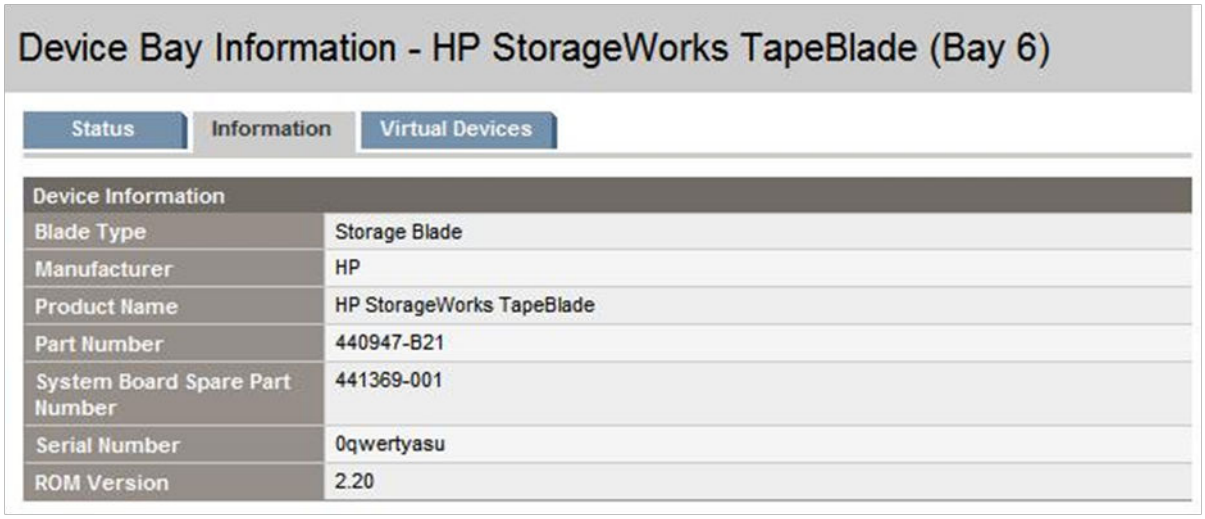
Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind

Zeile	Beschreibung
	oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Management Processor (Managementprozessor)	Status des Management-Schnittstellenprozessors des Speichercontrollers. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Temperature (Temperatur)	Die Temperatur liegt über der Warnschwelle. Mögliche Werte sind „OK“ oder „Temperature Warning“ (Warnung Temperatur).
Overheat Check (Überhitzungskontrolle)	Die Temperatur liegt über der Gefahrenschwelle. Mögliche Werte sind „OK“ und „Critical temperatur threshold reached“ (Kritischer Temperatur-Schwellenwert erreicht).
Power Allocation Request (Stromzuweisungsanforderung)	Die Stromversorgung für diesen Speicher-Blade ist unzureichend. Mögliche Werte sind „OK“ oder „Insufficient enclosure power“ (Unzureichende Stromversorgung des Gehäuses).
Cooling (Kühlung)	Die Anzahl der Lüfter reicht nicht aus, um diesen Speicher-Blade ordnungsgemäß zu kühlen, oder die Lüfterkonfiguration ist inkorrekt. Mögliche Werte sind „OK“ oder „Insufficient fans for enclosure cooling“ (Unzureichende Lüfter zur Kühlung des Gehäuses).
Device Location (Komponentenposition)	Konfigurationsstatus des Speicher-Blade-Einschubs. Mögliche Werte sind „OK“ und „Incorrect location for proper device cooling“ (Inkorrekte Position für angemessene Komponentenkühlung).
Device Operational (Komponente betriebsbereit)	Status des Speicher-Blade. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Degraded (Komponente beeinträchtigt)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Disk Tray (CD/DVD-Fach)	DVD Drive (CD/DVD-Laufwerk). Die möglichen Werte sind „Disk Tray is OPEN“ (CD/DVD-Fach ist OFFEN) oder „Disk Tray is CLOSED“ (CD/DVD-Fach ist GESCHLOSSEN).
Partner Device Presence (Vorhandensein einer gepaarten Komponenten)	Der Speicher-Blade besitzt einen mit ihm gepaarten Server. Neben ihm muss sich ein Server in der korrekten Konfiguration befinden. Mögliche Werte sind „OK“ oder „No adjacent partner found“ (Keine benachbarte gepaarte Komponente gefunden).
Power Sequence (Einschalt-Reihenfolge)	Der Speicher-Blade muss immer zuerst eingeschaltet werden. Wenn ein Speicher-Blade neben einem bereits eingeschalteten Server Blade eingesteckt wird, wird ihm die Stromversorgung verweigert. Damit der Speicher-Blade eingeschaltet wird, muss der Server Blade heruntergefahren werden. Anschließend kann der Server Blade wieder eingeschaltet wird. Mögliche Werte sind „OK“ oder „Potential partner device is already ON“ (Mögliche gepaarte Komponente ist bereits EINGESCHALTET).
Partner Device Link (Verknüpfung mit gepaarter Komponenten)	Ist die Leistung beeinträchtigt, wurden zwei Speicher-Blades nebeneinander im Gehäuse platziert. Mögliche Werte sind „OK“ oder „Inappropriate device in adjacent bay“ (Inkompatible Komponente im benachbarten Einschub).
Virtual Connect Configured (Virtuelle Verbindung konfiguriert)	Mögliche Werte sind „Configured for Virtual Connect“ (Für virtuelle Verbindung konfiguriert) oder „Not configured for Virtual Connect“ (Nicht für virtuelle Verbindung konfiguriert).

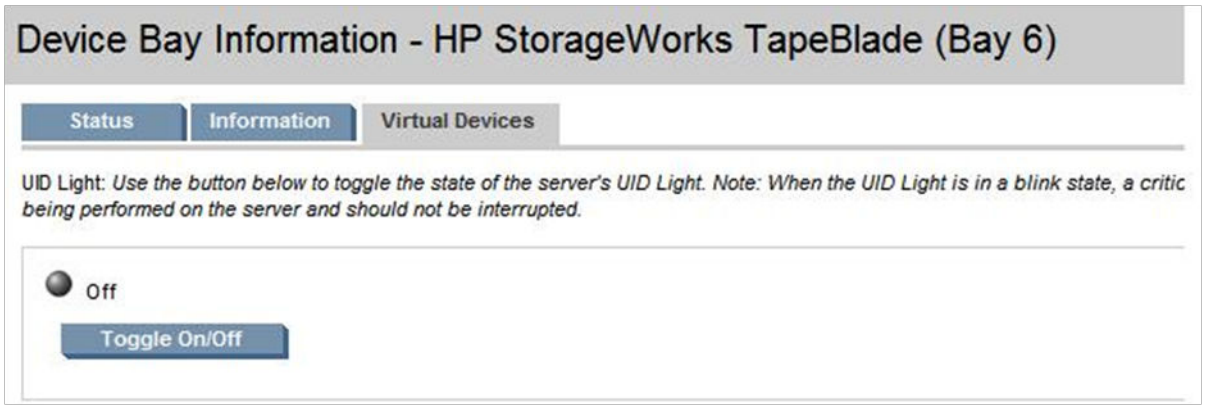
Informationen zu „Temperature Sensors“ (Temperaturfühler)

Spalte	Beschreibung
Standort	Ort des Sensors in der Komponente.

Spalte	Beschreibung
Status (Zustand)	Dies ist der Status des Temperatursensors. Der Status entspricht der grafischen Darstellung der Temperatur.
Temperature (Temperatur)	Grafische Darstellung der Temperatur.



Zeile	Beschreibung
Blade Type (Blade-Typ)	Der Typ der im Geräteeinschub installierten Komponente
Manufacturer (Hersteller)	Der Hersteller der im Geräteeinschub installierten Komponente
Product Name (Produktname)	Der allgemeine beschreibende Name des Server Blade
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatz-Server Blade zu verwendende Teilenummer
System Board Spare Part Number (Teilenummer der Ersatz-Systemplatine)	Die bei der Bestellung einer Ersatzteil-Systemplatine zu verwendende Teilenummer
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Server Blade
ROM Version (ROM-Version)	ROM-Versionsnummer.


Device Bay Information - HP StorageWorks TapeBlade (Bay 6)
Status
Information
Virtual Devices
UID Light: Use the button below to toggle the state of the server's UID Light. Note: When the UID Light is in a blink state, a critic
being performed on the server and should not be interrupted.
Off
Toggle On/Off

Die Blade-UID-LED für den Speicher-Blade wird über diesen Bildschirm ein- bzw. ausgeschaltet. Zum Umschalten der Blade-UID-LED klicken Sie auf **Toggle On/Off** (Ein-/Ausschalten).

Das Symbol direkt über der Schaltfläche „Toggle On/Off“ (Ein-/Ausschalten) ist grau, wenn die Blade-UID-LED inaktiv ist, und blau, wenn sie aktiv ist.

Informationen zum I/O-Erweiterungs-Blade

Durch Auswahl eines bestimmten I/O-Erweiterungs-Blade wird die Seite „Device Bay Information — Bay xx“ (Geräteeinschubs-Informationen – Einschub xx) geöffnet, wobei „xx“ der ausgewählte Einschub ist. Die in diesem Bildschirm angezeigten Informationen umfassen die Registerkarten „Status“, „Information“ und „Virtual Devices“ (Virtuelle Komponenten).

Registerkarte „Status“

Statusinformationen

Zeile	Beschreibung
Status (Zustand)	Der allgemeine Status des Blade. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Powered (Netzbetrieb)	Der Stromversorgungsstatus des Blade. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
Power Allocated (Zugewiesene Stromversorgung)	Die Menge der dem Blade zugewiesenen Stromversorgung in Watt.
Partner Device (Gepaarte Komponente)	Der Server Blade, mit dem der I/O-Erweiterungs-Blade gepaart ist.
Virtual Fan (Virtueller Lüfter)	Maximale Umdrehungen pro Minute (RPM) des virtuellen Lüfters in Prozent.

Die Informationen in der Statusinformationstabelle entsprechen dem Stand des letzten Downloads. Klicken Sie auf **Refresh** (Aktualisieren), um die Statusinformationen zu aktualisieren.

Diagnostic information (Diagnoseinformationen)

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Management Processor (Managementprozessor)	Status von iLO. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
I/O Configuration (I/O-Konfiguration)	Die Konfiguration des Geräteeinschubs ist inkorrekt. Wenn ein Speicher-Blade mit einem Server Blade voller Bauhöhe gepaart wird, und der Server Blade nicht über die richtige Mezzanine Card verfügt, hat dies eine ungültige I/O-Konfiguration zur Folge. Mögliche Werte sind „OK“ oder „I/O Mismatch Detected“ (I/O-Unstimmigkeit ermittelt).

Zeile	Beschreibung
Power Allocation Request (Stromzuweisungsanforderung)	Die Stromversorgung für diesen Blade ist unzureichend. Mögliche Werte sind „OK“ oder „Insufficient enclosure power“ (Unzureichende Stromversorgung des Gehäuses).
Cooling (Kühlung)	Die Anzahl der Lüfter reicht nicht aus, um diesen Server Blade ordnungsgemäß zu kühlen, oder die Lüfterkonfiguration ist falsch. Mögliche Werte sind „OK“ oder „Insufficient fans for enclosure cooling“ (Unzureichende Lüfter zur Kühlung des Gehäuses).
Device Location (Komponentenposition)	Der I/O-Blade wurde laut aktueller Lüfterkonfiguration in den falschen Steckplatz im Gehäuse eingebaut. Mögliche Werte sind „OK“ und „Incorrect location for proper device cooling“ (Inkorrekte Position für angemessene Komponentenkühlung).
Device Operational (Komponente betriebsbereit)	Komponente ist ausgefallen. Der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Degraded (Komponente beeinträchtigt)	Komponente ist ausgefallen. Der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Partner Device Presence (Vorhandensein einer gepaarten Komponenten)	Der I/O-Erweiterungs-Blade besitzt einen gepaarten Server. Neben ihm muss sich ein Server in der korrekten Konfiguration befinden. Mögliche Werte sind „OK“ oder „No adjacent partner found“ (Keine benachbarte gepaarte Komponente gefunden).
Power Sequence (Einschalt-Reihenfolge)	Der I/O-Erweiterungs-Blade muss immer zuerst eingeschaltet werden. Wenn ein I/O-Erweiterungs-Blade neben einem bereits eingeschalteten Server Blade eingesteckt wird, wird ihm die Stromversorgung verweigert. Der Server Blade muss ausgeschaltet werden, damit der I/O-Erweiterungs-Blade eingeschaltet werden kann, und dann kann der Server Blade wieder eingeschaltet werden. Mögliche Werte sind „OK“ oder „Potential partner device is already ON“ (Mögliche gepaarte Komponente ist bereits EINGESCHALTET).
Partner Device Link (Verknüpfung mit gepaarter Komponenten)	Mögliche Werte sind „OK“ oder „Inappropriate device in adjacent bay“ (Inkompatible Komponente im benachbarten Einschub). Diese Informationen werden nicht angezeigt, wenn der Server Blade nicht mit einem Speicher-/Erweiterungs-Blade gepaart ist.

Temperatursensoren

Spalte	Beschreibung
Sensor	Die Sensornummer.
Position	Ort des Sensors in der Komponente.
Status (Zustand)	Dies ist der Status des Temperatursensors. Der Status entspricht der grafischen Darstellung der Temperatur.
Temperature (Temperatur)	Grafische Darstellung der Temperatur.

Registerkarte mit den virtuellen Geräten des I/O-Erweiterungs-Blade

UID Light (UID-LED)

Bei Anklicken von **Toggle On/Off** (Ein-/Ausschalten) wird die UID-LED am I/O-Erweiterungs-Blade eingeschaltet (blau) bzw. ausgeschaltet (grau), um die Identifizierung des ausgewählten I/O-Erweiterungs-Blade zu erleichtern.

Registerkarte mit Informationen zum I/O-Erweiterungs-Blade

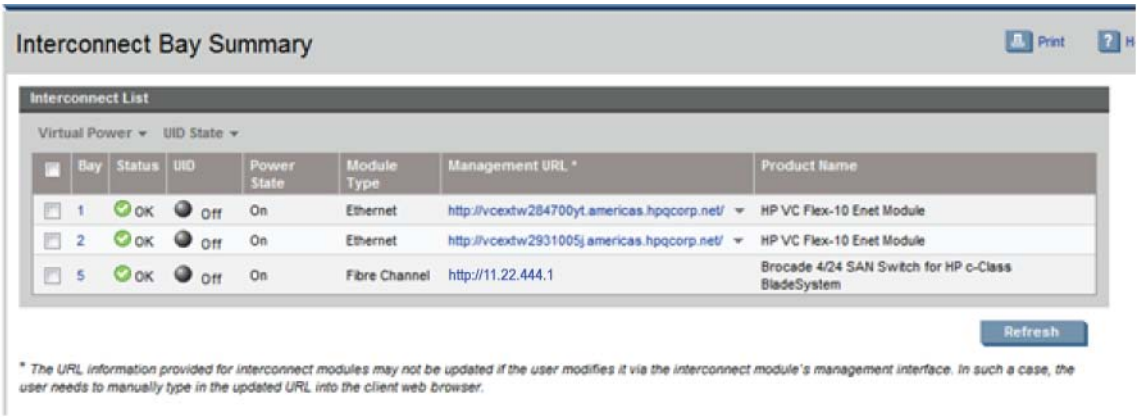
Device Information (Komponenteninformationen)

Zeile	Beschreibung
Blade Type (Blade-Typ)	I/O-Erweiterungs-Blade.
Manufacturer (Hersteller)	Name des Herstellerunternehmens des I/O-Erweiterungs-Blade.
Product Name (Produktname)	Allgemeiner beschreibender Name des I/O-Erweiterungs-Blade.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatz-I/O-Blade zu verwendende Teilenummer.
System Board Spare Part Number (Teilenummer der ErsatzSystemplatine)	Die bei der Bestellung einer zusätzlichen oder einer Ersatz-Systemplatine dieses Typs zu verwendende Teilenummer.
Serial Number (Seriennummer)	Eindeutige Seriennummer des I/O-Erweiterungs-Blade.
ROM Version (ROM-Version)	ROM-Versionsnummer.

Verbindungsmoduleinschübe

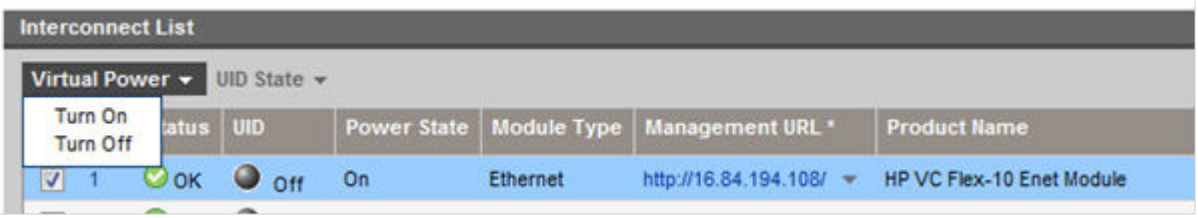
Bildschirm „Interconnect Bay Summary“ (Zusammenfassung der Verbindungsmoduleinschübe)

In der Kategorie „Interconnect Bays“ (Verbindungsmoduleinschübe) im Menü „Enclosure Information“ (Gehäuseinformationen) werden alle Verbindungsmodul-Komponenten innerhalb des Gehäuses aufgelistet. Bei Auswahl der Menüoption „Interconnect Bays“ (Verbindungsmoduleinschübe) wird direkt die Liste der Verbindungsmodul-Komponenten mit einer Tabelle geöffnet, aus der der Status einer jeden Verbindungsmodul-Komponenten innerhalb des Gehäuses sowie UID-Status, Stromversorgungsstatus, Modultyp, Management-URL und Produktname hervorgehen. Diese Parameter werden in der Tabelle nahe dem Ende dieses Abschnitts beschrieben.


Interconnect Bay Summary
Print
Interconnect List
Virtual Power
UID State
Bay
Status
UID
Power State
Module Type
Management URL *
Product Name
1 OK Off On Ethernet http://vcextw284700yt.americas.hpqcorp.net/ HP VC Flex-10 Enet Module
2 OK Off On Ethernet http://vcextw2931005j.americas.hpqcorp.net/ HP VC Flex-10 Enet Module
5 OK Off On Fibre Channel http://11.22.444.1 Brocade 4/24 SAN Switch for HP c-Class BladeSystem
Refresh
* The URL information provided for interconnect modules may not be updated if the user modifies it via the interconnect module's management interface. In such a case, the user needs to manually type in the updated URL into the client web browser.

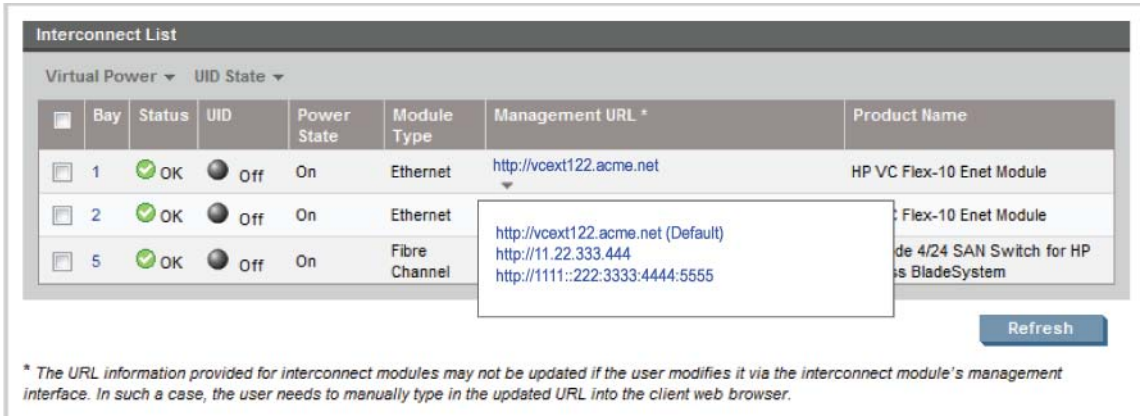
Mit dem Kontrollkästchen in der ersten Spalte auf der ersten Zeile werden die Kontrollkästchen für alle Verbindungsmodule aktiviert bzw. deaktiviert. Diese Funktion ist hilfreich, wenn Sie den UID-Status für alle Verbindungsmodule gleichzeitig umschalten möchten. Ansonsten enthält die erste Spalte die Kontrollkästchen, die zur Auswahl einzelner Verbindungsmodule aktiviert werden können. Nach Auswahl der gewünschten Verbindungsmodule können Sie über die Dropdown-Menüs „Virtual Power“ (Virtueller Netzschalter) oder „UID State“ (UID-Status) die entsprechende Aktion ausführen.

Ein Verbindungsmodul kann über das in der folgenden Abbildung dargestellte Menü „Virtual Power“ (Virtueller Netzschalter) ein- oder ausgeschaltet werden. HP empfiehlt, mit dieser Funktion nur jeweils eine Komponente ein- oder auszuschalten.



Das in der folgenden Abbildung dargestellte Menü „UID State“ (UID-Status) dient zum Einstellen der UID-LED am Verbindungsmodul. Das Einschalten der UID-LED erleichtert das Auffinden einer bestimmten Verbindungsmodule innerhalb eines Gehäuses. Diese LEDs lassen sich abhängig von den ausgewählten Kontrollkästchen einzeln oder gruppenweise ein- und ausschalten.

Klicken Sie zur Ansicht der verfügbaren Adressen-Links (IPv4 und IPv6) der Management Console auf den Abwärtspfeil neben der Management-URL-Adresse. Wie in der folgenden Abbildung dargestellt wird ein Popup-Fenster angezeigt. Wenn die FQDN-Link-Unterstützung aktiviert ist und bestimmten DNS-Konfigurationsanforderungen entsprochen wird, wird als Standard-Management-URL eine FQDN-basierte-Adresse angezeigt (wie dargestellt). Weitere Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).



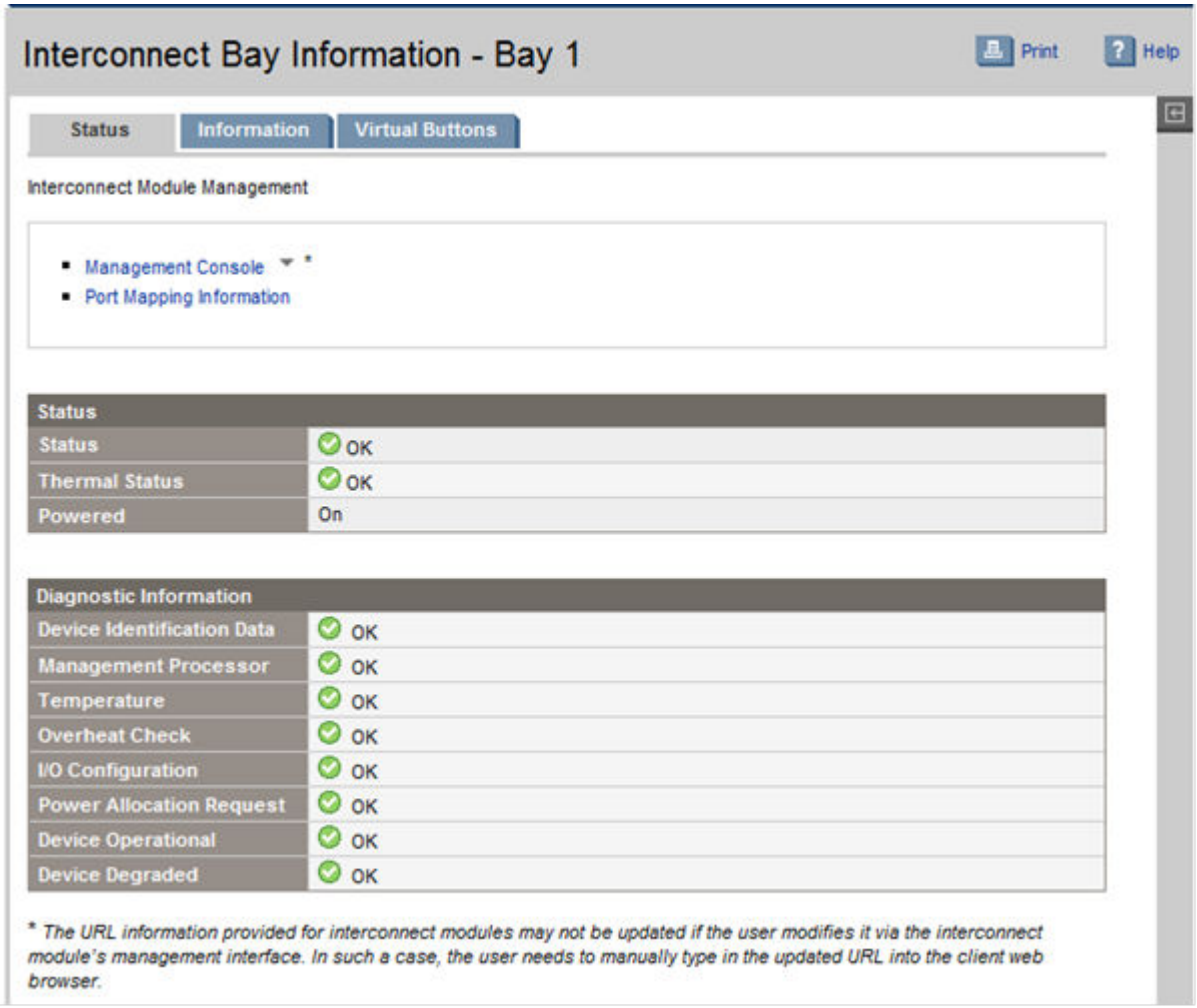
Spalte	Beschreibung
Kontrollkästchen	Klicken Sie auf die Kontrollkästchen neben dem Einschub bzw. den Einschüben, auf die die Funktionen „Virtual Power“ (Virtueller Netzschalter) und „UID“ angewandt werden sollen.
Bay (Einschub)	Einschub im Gehäuse des entsprechenden Verbindungsmoduls. Dieses Feld zeigt nur bestückte Einschübe an. Leere Einschübe werden nicht in dieser Tabelle nicht angezeigt.
Status (Zustand)	Der allgemeine Status des Verbindungsmoduls. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).

Spalte	Beschreibung
UID	Der Status der UID am Verbindungsmodul. Mögliche Werte sind „On“ (blau) oder „Off“ (grau).
Power State (Stromversorgungsstatus)	Der Stromversorgungsstatus des Verbindungsmoduls. Mögliche Werte sind „On“ (Ein) oder „Off“ (Aus).
Module Type (Modultyp)	Netzwerkschnittstellentyp des in diesem Einschub installierten Verbindungsmoduls. Mögliche Werte sind „Ethernet“ oder „Fiber“.
Management URL (Verwaltungs-URL)	IPv4-Adresse, über die das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann. Um die verfügbare Verwaltungs-URL-Adressen-Verbindungen (IPv4 und IPv6) anzuzeigen, klicken Sie auf den Abwärtspfeil, um ein Dropdown-Menü anzuzeigen. Wenn die FQDN-Link-Unterstützung aktiviert ist und bestimmten DNS-Konfigurationsanforderungen entsprochen wird, wird als Standard-Management-URL eine FQDN-basierte-Adresse angezeigt. Weitere Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).
Product Name (Produktname)	Allgemeiner beschreibender Name des Verbindungsmoduls.

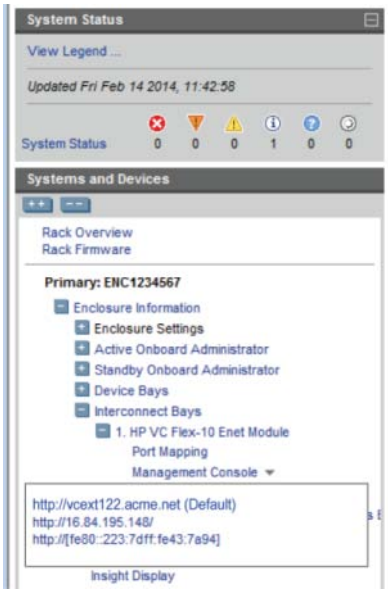
Die Informationen auf dieser Seite entsprechen dem letzten Download. Um die aktualisierten Informationen anzuzeigen, klicken Sie auf **Refresh** (Aktualisieren).

Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub)

Im Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub) werden Informationen über die Einschübe angezeigt, in die Switches und Router eingebaut werden können. Darüber hinaus können Sie die Onboard Administrator-Module anzeigen.



Klicken Sie zum Herstellen einer Verbindung zur Management Console auf den Link **Management Console**. Klicken Sie zur Ansicht der verfügbaren Adressen-Links (IPv4 und IPv6) der Management Console auf den Abwärtspfeil neben dem Link. Sie können auch über die Navigationsstruktur eine Verbindung zur Management Console herstellen, wie in der folgenden Abbildung dargestellt. Wenn die FQDN-Link-Unterstützung aktiviert ist und bestimmten DNS-Konfigurations-Anforderungen entsprochen wird, wird in beiden Fällen als Standard-Link eine FQDN-basierte Adresse angezeigt. Weitere Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).



Um Informationen zur Portzuordnung auf dem von Ihnen ausgewählten Verbindungsmoduleinschub anzuzeigen, klicken Sie auf den Link **Port Mapping Interconnect** (Portzuordnung des Verbindungsmoduls). Die Portzuordnungsinformationen können auch aus der Navigationsstruktur ausgewählt werden.

Statusinformationen

Zeile	Beschreibung
Status (Zustand)	Der allgemeine Zustand des Verbindungsmoduls. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Thermal Status (Thermischer Status)	Der thermische Status des Verbindungsmoduls. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Failed“ (Fehler).
Powered (Netzbetrieb)	Der Stromversorgungsstatus des Blade. Mögliche Werte sind „On“ (Ein), „Off“ (Aus) und „Delayed“ (Verzögert).
Power Delay Remaining (Verbleibende Stromzufuhrverzögerung)	Die Anzahl der Sekunden, die verbleiben, bevor die Komponente eingeschaltet wird.

Diagnostic information (Diagnoseinformationen)

Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Management Processor (Managementprozessor)	Der Managementprozessor antwortet nicht. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Temperature (Temperatur)	Die Temperatur liegt über der Warnschwelle. Mögliche Werte sind „OK“ oder „Temperature Warning“ (Warnung Temperatur).

Zeile	Beschreibung
Overheat Check (Überhitzungskontrolle)	Die Temperatur liegt über der Gefahrenschwelle. Mögliche Werte sind „OK“ und „Critical temperatur threshold reached“ (Kritischer Temperatur-Schwellenwert erreicht).
I/O Configuration (I/O-Konfiguration)	Die Konfiguration des Verbindungsmoduleinschubs ist inkorrekt. Mögliche Werte sind „OK“ oder „I/O Mismatch“ (I/O-Unstimmigkeit).
Power Allocation Request (Stromzuweisungsanforderung)	Die Stromversorgung für dieses Verbindungsmodul ist unzureichend. Mögliche Werte sind „OK“ oder „Insufficient enclosure power“ (Unzureichende Stromversorgung des Gehäuses).
Device Operational (Komponente betriebsbereit)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Degraded (Komponente beeinträchtigt)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Informational (Geräteinformationen)	Das Gerät funktioniert normal, erfordert jedoch Aufmerksamkeit.
Duplicate IP Address (Doppelte IP-Adresse)	Eine Kontrolle während der Zuweisung, ob im Netzwerk eine doppelte IP-Adresse vorhanden ist. Mögliche Werte sind „OK“ oder eine informative Meldung, dass im Netzwerk eine doppelte IP-Adresse vorhanden ist.

Registerkarte „Interconnect Bay Information“ (Informationen zum Verbindungsmoduleinschub)

Hardwareinformationen

Zeile	Beschreibung
Product Name (Produktname)	Der allgemeine beschreibende Name des Verbindungsmoduls.
Management IP Address (Management-IP-Adresse)	Die IP-Adresse der Verbindungsmodul-Management-Oberfläche.
Management URL (Verwaltungs-URL)	Adresse, über die das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann.
User Assigned Name (Vom Benutzer zugewiesener Name)	Ein vom Benutzer dem Verbindungsmodul zugewiesener Name. Sofern unterstützt, wird der Name über die Verbindungsmodul-Management-Oberfläche zugewiesen.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen Verbindungsmoduls dieses Typs zu verwendende Teilenummer.
Spare Part Number (Ersatzteilnummer)	Die bei der Bestellung eines Ersatzteil-Verbindungsmoduls dieses Typs zu verwendende Teilenummer.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Verbindungsmoduls.
Typ	Der Schnittstellentyp des Verbindungsmoduls. Mögliche Werte sind „Ethernet“ oder „Fiber“.
Manufacturer (Hersteller)	Der Name des Herstellerunternehmens des Verbindungsmoduls.
Temperature Sensor (Temperatursensor)	Zeigt an, ob das Verbindungsmodul über einen Temperatursensor verfügt.

Zeile	Beschreibung
Firmware Version (Firmwareversion)	Die Firmwareversion des Verbindungsmoduls.
VLAN ID (Name)	VLAN-ID-Nummer und -Name, die dem Verbindungsmoduleinschub zugewiesen wurden.

IPv6-Informationen

Zeile	Beschreibung
Link Local Address (Lokale Verbindungsadresse)	Die lokale IPv6-Verbindungsadresse der Verbindungsmodulschnittstelle.
EBIPA Address (EBIPA-Adresse)	Die EBIPA-IPv6-Adresse der Verbindungsmodulschnittstelle.
DHCPv6 Address (DHCPv6-Adresse)	Die DHCP-IPv6-Adresse der Verbindungsmodulschnittstelle.
SLAAC Address (SLAAC-Adresse)	Die SLAAC-IPv6-Adresse der Verbindungsmodulschnittstelle.
Lokaler Verbindungsmanagement-URL	Der lokale IPv6-Verbindungsmanagement-URL, über den das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann.
EBIPA-Management-URL	Der EBIPA-IPv6-Management-URL, über den das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann.
DHCPv6-Management-URL	Der DHCP-IPv6-Management-URL, über den das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann.
SLAAC-Management-URL	Der SLAAC-IPv6-Management-URL, über den das Verbindungsmodul zur Verwendung im Netzwerk verwaltet und konfiguriert werden kann.

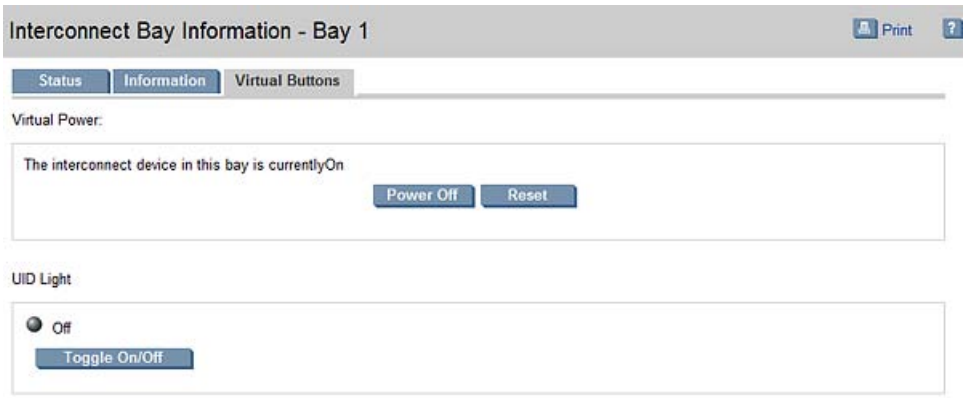
Verbindungsinformationen

Zeile	Beschreibung
JS2 Connector (JS2-Anschluss)	Dieses Feld zeigt an, ob der JS2-Anschluss vorhanden ist oder nicht.
Internal Ethernet Interface to OA (Interne Ethernet-Schnittstelle zu OA)	Dieses Feld zeigt an, ob eine interne Ethernet-Schnittstelle zu Onboard Administrator vorhanden ist oder nicht.
Internal Ethernet Route to OA (Interner Ethernet-Leitweg zu OA)	Dieses Feld zeigt den Status eines internen Ethernet-Leitwegs zu Onboard Administrator an. Mögliche Werte sind „Enabled“ (Aktiviert) oder „Disabled“ (Deaktiviert).
Internal Serial Interface to OA (Interne serielle Schnittstelle zu OA)	Dieses Feld zeigt an, ob eine interne serielle Ethernet-Schnittstelle zu Onboard Administrator vorhanden ist oder nicht.
Internal Serial Route to OA (Interner Leitweg zu OA)	Dieses Feld zeigt den Status eines internen seriellen Leitwegs zu Onboard Administrator an. Mögliche Werte sind „Enabled“ (Aktiviert) oder „Disabled“ (Deaktiviert).
Serial Port Baud Rate (Baudrate des seriellen Anschlusses)	Dieses Feld zeigt die Baudrate des seriellen Anschlusses an.

Zeile	Beschreibung
External Serial Port Interface (Externe serielle Anschluss-Schnittstelle)	Dieses Feld zeigt an, ob eine externe serielle Anschluss-Schnittstelle vorhanden ist oder nicht.
External Ethernet Interface (Externe Ethernet-Schnittstelle)	Dieses Feld zeigt an, ob eine externe Ethernet-Schnittstelle vorhanden ist oder nicht.

Virtuelle Tasten des Verbindungsmoduleinschubs

Mit den virtuellen Tasten des Verbindungsmoduleinschubs können Sie die Stromversorgung steuern, zurücksetzen oder die UID am Modul über die grafische Benutzeroberfläche von Onboard Administrator ein- und ausschalten.

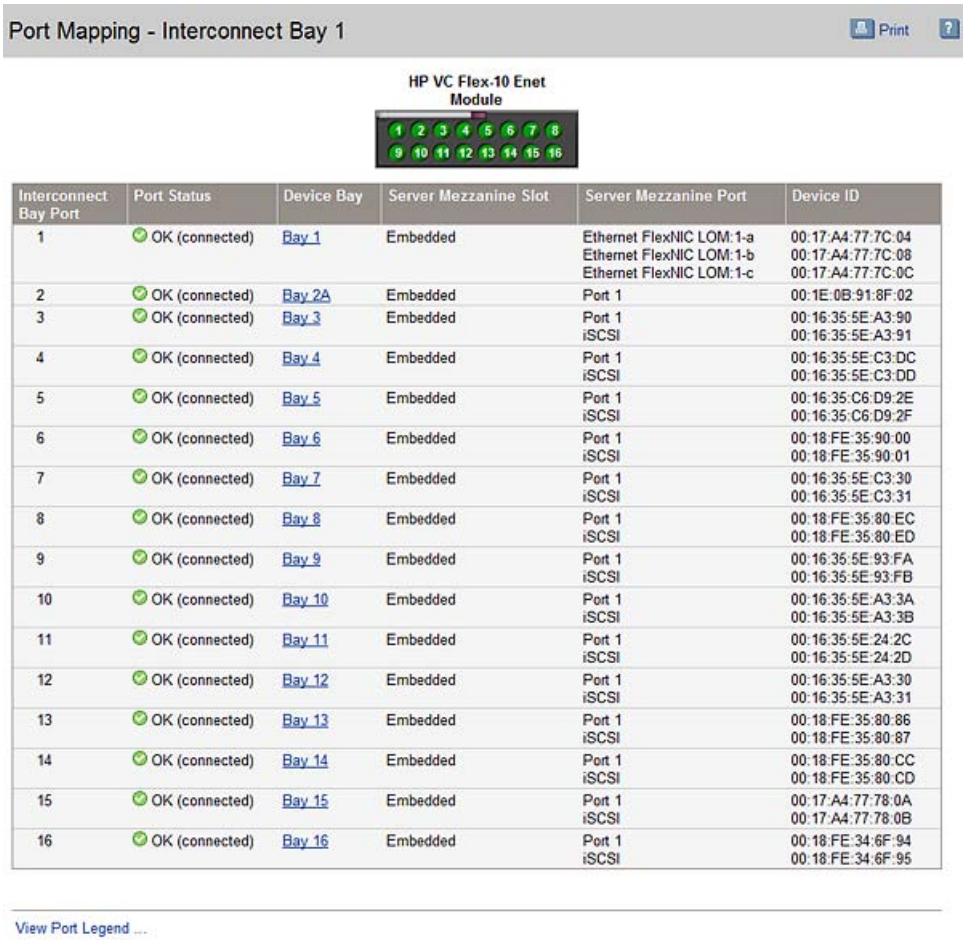


Schaltfläche	Beschreibung
Power Off (Ausschalten)	Durch Klicken auf diese Schaltfläche wird das Verbindungsmodul ausgeschaltet.
Reset (Zurücksetzen)	Durch Klicken auf diese Schaltfläche wird das Verbindungsmodul heruntergefahren und anschließend wieder eingeschaltet, und somit zurückgesetzt.
Toggle On/Off (Ein-/Ausschalten)	Durch Klicken auf diese Schaltfläche wird die UID am Verbindungsmodul eingeschaltet (blau) oder ausgeschaltet (grau), um die Identifikation des ausgewählten Verbindungsmoduls zu erleichtern.

HINWEIS: Ausgeschaltete Verbindungsmodule werden nach einem Neustart des Onboard Administrators eingeschaltet oder es findet ein Failover des Moduls statt, wenn wenn die Stromversorgung des Gehäuses dafür ausreicht.

Bildschirm „Interconnect Bay Port Mapping“ (Portzuordnung des Verbindungsmoduleinschubs)

Im Bildschirm „Interconnect Bay Port Mapping“ (Portzuordnung des Verbindungsmoduleinschubs) wird eine grafische Ansicht und eine Tabellenansicht der Portzuordnung für den Verbindungsmoduleinschub angezeigt.


Port Mapping - Interconnect Bay 1
Print
HP VC Flex-10 Enet Module
1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
Interconnect Bay Port | Port Status | Device Bay | Server Mezzanine Slot | Server Mezzanine Port | Device ID
1 | OK (connected) | Bay 1 | Embedded | Ethernet FlexNIC LOM:1-a
Ethernet FlexNIC LOM:1-b
Ethernet FlexNIC LOM:1-c | 00:17:A4:77:7C:04
00:17:A4:77:7C:08
00:17:A4:77:7C:0C
2 | OK (connected) | Bay 2A | Embedded | Port 1 | 00:1E:0B:91:8F:02
3 | OK (connected) | Bay 3 | Embedded | Port 1
iSCSI | 00:16:35:5E:A3:90
00:16:35:5E:A3:91
4 | OK (connected) | Bay 4 | Embedded | Port 1
iSCSI | 00:16:35:5E:C3:DC
00:16:35:5E:C3:DD
5 | OK (connected) | Bay 5 | Embedded | Port 1
iSCSI | 00:16:35:C6:D9:2E
00:16:35:C6:D9:2F
6 | OK (connected) | Bay 6 | Embedded | Port 1
iSCSI | 00:18:FE:35:90:00
00:18:FE:35:90:01
7 | OK (connected) | Bay 7 | Embedded | Port 1
iSCSI | 00:16:35:5E:C3:30
00:16:35:5E:C3:31
8 | OK (connected) | Bay 8 | Embedded | Port 1
iSCSI | 00:18:FE:35:80:EC
00:18:FE:35:80:ED
9 | OK (connected) | Bay 9 | Embedded | Port 1
iSCSI | 00:16:35:5E:93:FA
00:16:35:5E:93:FB
10 | OK (connected) | Bay 10 | Embedded | Port 1
iSCSI | 00:16:35:5E:A3:3A
00:16:35:5E:A3:3B
11 | OK (connected) | Bay 11 | Embedded | Port 1
iSCSI | 00:16:35:5E:24:2C
00:16:35:5E:24:2D
12 | OK (connected) | Bay 12 | Embedded | Port 1
iSCSI | 00:16:35:5E:A3:30
00:16:35:5E:A3:31
13 | OK (connected) | Bay 13 | Embedded | Port 1
iSCSI | 00:18:FE:35:80:86
00:18:FE:35:80:87
14 | OK (connected) | Bay 14 | Embedded | Port 1
iSCSI | 00:18:FE:35:80:CC
00:18:FE:35:80:CD
15 | OK (connected) | Bay 15 | Embedded | Port 1
iSCSI | 00:17:A4:77:78:0A
00:17:A4:77:78:0B
16 | OK (connected) | Bay 16 | Embedded | Port 1
iSCSI | 00:18:FE:34:6F:94
00:18:FE:34:6F:95
View Port Legend ...

Grafische Ansicht

Wenn Sie den Cursor über den Port des Verbindungsmoduleinschubs halten, zeigt die grafische Ansicht die gleichen Informationen an, die auch in der Tabellenansicht zu sehen sind.

Tabellenansicht

Spalte	Beschreibung
Interconnect Bay Port (Port für Verbindungsmoduleinschub)	Die Nummer des Ports für den Verbindungsmoduleinschub in der Reihenfolge 1 bis 16.
Port Status (Port-Status)	Der aktuelle Status des Ports.
Device Bay (Geräteeinschub)	Der Geräteeinschub, der der Portzuordnung des Verbindungsmoduls entspricht.
Server Mezzanine Slot (Server-Mezzanine-Steckplatz)	Der Komponententyp, der in das Mezzanine des Server Blade eingebaut wurde.
Server Mezzanine Port (Server-Mezzanine-Port)	Der physikalische Port der Mezzanine-Komponente.
Device ID (Komponenten-ID)	Die MAC-Adresse des Ports für den Verbindungsmoduleinschub.

Gehäuse-Power Management

Planung für das Power Management

Die Netzteilgehäuse enthalten jeweils sechs Netzteile, die direkt von Onboard Administrator überwacht werden. Es können bis zu zwei Netzteilgehäuse mit einem einzelnen Gehäuse verbunden werden.

Onboard Administrator ist für die Berechnung des Redundanzstatus, der verfügbaren Gesamtstrom und des Gesamtstromverbrauchs verantwortlich. Diese Informationen werden dem Benutzer angezeigt, und dienen zur Verwaltung der Stromressourcen. Die Anzeigen des Stromversorgungs-Subsystems von Onboard Administrator zeigen den Status und Informationen für jedes Netzteil sowie für das Netzteilgehäuse selbst an.

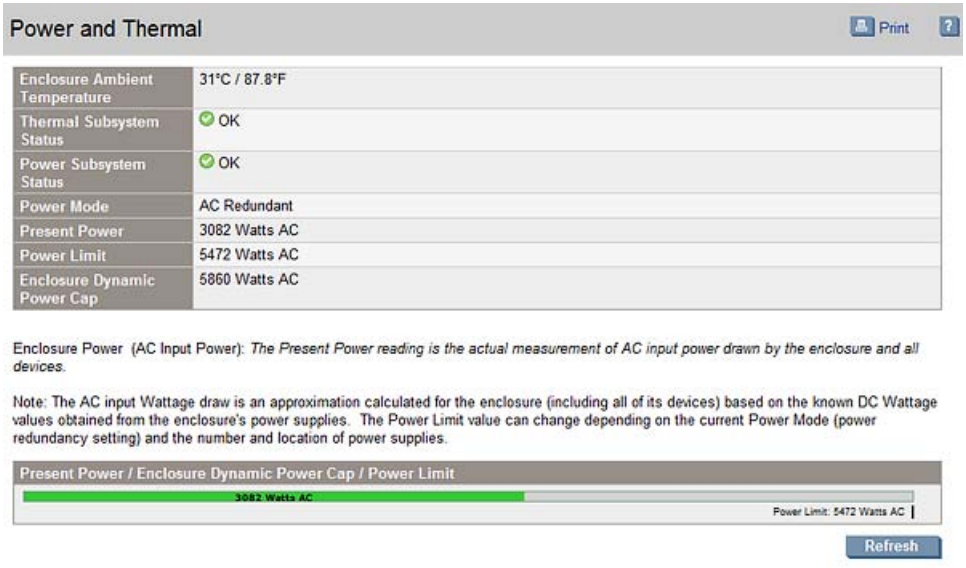
Im Bereich der Netzfehlerüberwachung liegt auch die Steuerung von elektronischen Sicherungen zwischen der Netzteil-Rückwandplatine und den Server- oder Switch-Einschüben. Der Onboard Administrator sendet einen Alarm beim Ausfallen von Sicherungen, damit diese manuell zurückgesetzt werden können.

Bei der Installation zusätzlicher Netzteile im Gehäuse werden im selben Gehäuse keine unterschiedlichen Netzteil-Teilenummern unterstützt. Onboard Administrator weist mit einem entsprechenden Symbol darauf hin, welche Netzteile ersetzt werden müssen.

HINWEIS: HP 1200W Common Slot Silver Hotplug-Netzteile, Ersatzteilenummern 441830-001 und 498152-001, können in einem Gehäuse miteinander kombiniert werden und werden gleichwertig behandelt.

Informationen zur korrekten Installation der Netzteile im Gehäuse finden Sie im betreffenden HP BladeSystem c7000-Gehäuse Setup- und Installationshandbuch.

Bildschirm „Power and Thermal“ (Stromversorgung und Wärmewerte)


Power and Thermal
Print
Enclosure Ambient Temperature
31°C / 87.8°F
Thermal Subsystem Status
OK
Power Subsystem Status
OK
Power Mode
AC Redundant
Present Power
3082 Watts AC
Power Limit
5472 Watts AC
Enclosure Dynamic Power Cap
5860 Watts AC
Enclosure Power (AC Input Power): The Present Power reading is the actual measurement of AC input power drawn by the enclosure and all devices.
Note: The AC input Wattage draw is an approximation calculated for the enclosure (including all of its devices) based on the known DC Wattage values obtained from the enclosure's power supplies. The Power Limit value can change depending on the current Power Mode (power redundancy setting) and the number and location of power supplies.
Present Power / Enclosure Dynamic Power Cap / Power Limit
3082 Watts AC
Power Limit: 5472 Watts AC
Refresh

Zeile	Beschreibung
Enclosure Ambient Temperature (Gehäuseumgebungstemperatur)	Dieses Feld zeigt die höchste, von den installierten Blade-Komponenten gemeldete Umgebungstemperatur an. Sind keine Blade-Komponenten installiert, zeigt dieses

Zeile	Beschreibung
	Feld die Temperatur des Onboard Administrator-Moduls als eine Annäherung an die Umgebungstemperatur an.
Thermal Subsystem Status (Status des thermischen Subsystems)	Der allgemeine Wärmestatus des Gehäuses. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Power Subsystem Status (Status des Stromversorgungs-Subsystems)	Der allgemeine Stromversorgungsstatus des Gehäuses Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Power Mode (Stromversorgungsmodus)	Eine Benutzereinstellung zur Konfiguration der Gleichstromkapazität des Gehäuses und der Redundanz der Stromzufuhr des Gehäuses. Mögliche Werte werden unter „Power-Management“ aufgeführt.
Present Power (Aktueller Verbrauch)	Die Menge des von allen Komponenten im Gehäuse verbrauchten Stroms in Watt.
Power Limit (Strombegrenzung)	Der für den Verbrauch des Gehäuses maximal verfügbare Strom, gemessen in Watt.
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Eine für eine Gruppe von Servern im Gehäuse festgelegte Stromobergrenze. Wenn die Server ausgeführt werden, ändert sich der Strombedarf für jeden Server. Für jeden Server wird eine Stromobergrenze festgelegt, um den Server mit genug Strom zu versorgen, damit er seine Arbeitsauslastungsanforderungen erfüllen kann, während er gleichzeitig die dynamische Stromobergrenze des Gehäuses einhält. Durch kontinuierliche Überwachung des Strombedarfs und automatische Regulierung der Server-Stromobergrenzen wird sichergestellt, dass die Leistung nur minimal beeinträchtigt wird. Angaben zur Funktion „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) werden nur angezeigt, sofern eine Obergrenze definiert wurde.

Present Power/Enclosure Dynamic Power Cap/Power Limit (Aktueller Verbrauch/Dynamische Stromobergrenze des Gehäuses/Strombegrenzung)

Der Wert für „Present Power“ (Aktueller Verbrauch) stellt den Strom in Watt dar, der von allen Komponenten im Gehäuse verbraucht wird. Die Funktion „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) reguliert automatisch Stromobergrenzen auf Servern im Gehäuse, um Arbeitsauslastungsanforderungen auf Servern zu erfüllen, während gleichzeitig die dynamische Stromobergrenze des Gehäuses eingehalten wird. Der Wert für „Power Limit“ (Strombegrenzung) ist die maximale Menge an Eingangsstrom, die zum Verbrauch durch das Gehäuse verfügbar ist. Dieser Wert ist von der Stromversorgungs-Redundanzeinstellung des Gehäuses und der Anzahl und Position der Netzteile im Gehäuse abhängig. Wurde ein Wert für „Static Power Limit“ (Statische Strombegrenzung) angegeben, zeigt die Strombegrenzung dieses Limit an.

Power Management

Zum Einstellen der Stromversorgungs-Verwaltungsoptionen in Onboard Administrator gehen Sie zu dem Menü auf der linken Seite und wählen das zu verwaltende Gehäuse aus. Klicken Sie auf **Power and Thermal>Power Management** (Stromversorgung und Wärmewerte>Stromversorgungsverwaltung). Die Power Management-Hauptseite wird mit den folgenden Optionen angezeigt:

- AC Redundant (Netzredundant)
- Power Supply Redundant (Netzteilredundant)
- Not Redundant

Unter den Hauptoptionen für das Power Management befindet sich das Kontrollkästchen „Enable Dynamic Power“ (Dynamischen Stromsparmodus aktivieren), mit dem Sie den dynamischen Energiesparmodus aktivieren oder deaktivieren können.

Mit dem Feld „AC Input VA Limit“ (Grenzwert für Eingangsleistung) können Sie den VA-Grenzwert für das Gehäuse einstellen. Nach Erreichung dieses Grenzwerts durch das Gehäuse können keine weiteren Blades, Netzteile, Lüfter oder Switches eingeschaltet werden. Wird ein Wert in das Feld für den VA-Grenzwert eingegeben, der niedriger ist als die aktuell verwendete VA-Zahl für das Gehäuse, schaltet das Gehäuse keine Komponenten innerhalb dieses Gehäuses aus. Wird jedoch eine Komponente ausgeschaltet, kann sie aufgrund der Regel für den VA-Grenzwert nicht mehr eingeschaltet werden, die in den Stromverwaltungseinstellungen von Onboard Administrator festgelegt wurde.

HINWEIS: Wenn als Redundanzmodus „Redundant“, „AC Redundant“ (Netzredundant) oder „Power Supply Redundant“ (Netzteilredundant) eingestellt ist und die Stromversorgungsredundanz verloren geht, müssen Sie entweder zusätzliche Netzteile hinzufügen oder die Einstellung für den Redundanzmodus in Onboard Administrator ändern, um den Status des Stromversorgungs-Subsystems wiederherzustellen. Korrektive Maßnahmen sind im Insight Display zu finden.

HINWEIS: Um den Stromredundanzmodus zu ändern, müssen Sie die dynamische Stromobergrenze des Gehäuses deaktivieren. Setzen Sie die dynamische Stromobergrenze des Gehäuses nach Ändern des Stromredundanzmodus auf die neuen Bereiche zurück.

Stromverwaltungsoptionen

Die Stromverwaltungssysteme der HP BladeSystem c3000- und c7000-Gehäuse ermöglichen Ihnen, Ihr Gehäuse gemäß Ihren Anforderungen zu konfigurieren. Auf dem Bildschirm „Onboard Administrator Power Management“ (Onboard Administrator-Stromversorgungsverwaltung) stehen unterschiedliche Stromverwaltungsoptionen zur Auswahl. Diese Stromverwaltungsoptionen werden in der folgenden Tabelle beschrieben.

Stromverwaltungsoption	Insight Display-Name	Beschreibung
Stromversorgungsmodus (Redundanzmodus)		
„Redundant“ oder „AC Redundant“ (Wechselstromredundant)	„Redundant“ oder „AC Redundant“ (Wechselstromredundant)	Der OA erkennt den Typ der vorhandenen Netzteile, passt das Verhalten des Stromversorgungsmodus automatisch entsprechend an und zeigt die zugehörige Modusbezeichnung an: • Wenn Gleichstromnetzteile vorhanden sind: Modus „Redundant“ • Wenn Wechselstromnetzteile vorhanden sind: Modus „AC Redundant“ (Wechselstromredundant) Wird auch als N+N-Redundanz oder Stromnetzredundanz bezeichnet. *N* Netzteile werden zur Stromversorgung und *N* Netzteile werden zur Sicherung der Redundanz verwendet (dabei kann *N* 1, 2 oder 3 sein). Es können bis zu drei Netzteile ausfallen, ohne dass das Gehäuse ausfällt. Bei korrekter Verdrahtung mit redundanten AC- und DC-Zuleitungen stellt diese Konfiguration auch sicher, dass das Gehäuse bei einem Ausfall einer AC- oder DC-Zuleitung nicht ausgeschaltet wird. Sollte der unwahrscheinliche Fall eintreten, dass mehr als ein Netzteil aufgrund von Ausfällen mehrerer Netzteile oder des Stromnetzes keinen Strom mehr liefern kann, dann wird das System möglicherweise ausgeschaltet. Das System wird ausgeschaltet, wenn der Strom, der von den noch

Stromverwaltungsoption	Insight Display-Name	Beschreibung
		funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt.
Power Supply Redundant (Netzteilredundant)	Power Supply (Netzteil)	Für alle Netzteile. Dieser Modus unterstützt zwei bis sechs Netzteile. Dies wird auch als N+1-Redundanz bezeichnet. Bei diesem Stromversorgungsmodus liefern *N* Netzteile den Strom und 1 Netzteil sichert die Redundanz (dabei kann *N* 1, 2, 3, 4 oder 5 sein). Wenn ein 3-Phasen-Stromeingangsmodul für das c7000 Gehäuse verwendet wird, empfiehlt HP 3 oder 6 aktive Netzteile (2+1 oder 5+1) für einen ordnungsgemäßen Phasenausgleich. Dieser Stromversorgungsmodus soll das System entwurfsgemäß bei Ausfall eines Netzteils schützen. Sollte der unwahrscheinliche Fall eintreten, dass mehr als ein Netzteil aufgrund von Ausfällen mehrerer Netzteile oder des Stromnetzes keinen Strom mehr liefern kann, dann wird das System möglicherweise ausgeschaltet. Das System wird ausgeschaltet, wenn der Strom, der von den noch funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt.
Not Redundant (Nicht redundant)	Keine	Für alle Netzteile. Dieser Modus unterstützt 1 bis 6 Netzteile. Bei diesem Stromversorgungsmodus liefern *N* Netzteile den Strom und kein Netzteil sichert die Redundanz (dabei kann *N* 1, 2, 3, 4, 5 oder 6 sein). Wenn ein 3-Phasen-Stromeingangsmodul für das c7000 Gehäuse verwendet wird, empfiehlt HP 3 oder 6 aktive Netzteile für einen ordnungsgemäßen Phasenausgleich. Es ist keine Stromversorgungsredundanz gegeben und es werden keine entsprechenden Warnungen ausgegeben. Wenn ein Netzteil aufgrund eines Ausfalls des Netzteils oder des Stromnetzes keinen Strom mehr liefern kann, wird das System möglicherweise ausgeschaltet. Es wird ausgeschaltet, wenn der Strom, der von den noch funktionierenden Netzteilen bereitgestellt wird, die Stromversorgungsanforderungen des Systems nicht erfüllt. Dieser Stromversorgungsmodus wird für bereitgestellte Systeme in Produktionsumgebungen nicht empfohlen.
Modus „Dynamic Power“ (Dynamische Stromversorgung) (aktiviert oder deaktiviert)		
Dynamic Power (Dynamischer Stromsparmodus)	Dynamic Power (Dynamischer Stromsparmodus)	Bei Aktivierung versetzt der dynamische Stromsparmodus ungenutzte Netzteile automatisch in den Standbymodus, um die Netzteileffizienz des Gehäuses zu erhöhen und dadurch den Stromverbrauch des Gehäuses bei niedrigem Strombedarf zu verringern. Bei erhöhtem Strombedarf wird die volle Leistung von Netzteilen im Standbymodus automatisch wiederhergestellt. Weitere Informationen über die dynamische Stromversorgung folgen dieser Tabelle.
Modus „Power Limit“ (Strombegrenzung)		
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Keine	Ermöglicht die Angabe eines Limits für den Stromverbrauch des Gehäuses. Die Leistungsaufnahme wird begrenzt, indem Stromobergrenzen von Server Blades dynamisch so verwaltet werden, dass die Gesamtstromobergrenze des Gehäuses nicht

Stromverwaltungsoption	Insight Display-Name	Beschreibung
		überschritten wird. Weitere Informationen finden Sie in der nachstehenden Tabelle zur Strombegrenzung.
Static Power Limit (Statische Strombegrenzung)	Power Limit (Strombegrenzung)	Eine optionale Einstellung zur Strombegrenzung. Jedes Mal, wenn Sie versuchen, eine Komponente einzuschalten, werden der gesamte Strombedarf der neuen Komponente sowie der bereits eingeschalteten Komponenten mit dieser statischen Strombegrenzung verglichen. Überschreitet der gesamte Strombedarf den Grenzwert, wird das Einschalten der neuen Komponente verhindert. Weitere Informationen über die statische Strombegrenzung und worin sie sich von der dynamischen Stromobergrenze des Gehäuses unterscheidet, finden Sie in der nachstehenden Tabelle zur Strombegrenzung.

HINWEIS: Unabhängig von dem aktivierten Redundanzmodus sind alle im Gehäuse vorhandenen betriebsfähigen Netzteile in der Regel aktiv und tragen zur Deckung des Strombedarfs des Gehäuses bei. Wenn der Modus der dynamischen Stromversorgung aktiviert ist, werden einige Netzteile möglicherweise automatisch in den Standbymodus geschaltet, um die Gesamteffizienz der Stromversorgung des Gehäuses zu steigern. Weitere Informationen finden Sie in der nachstehenden Beschreibung des Modus der dynamischen Stromversorgung.

Mit Onboard Administrator kann der eingestellte Stromversorgungsmodus (Redundanz) geändert werden, nachdem das Gehäuse und die Geräte eingeschaltet wurden. Wenn der Stromversorgungsmodus geändert wird, aktualisiert Onboard Administrator bei Bedarf den Redundanzstatus und meldet beeinträchtigte bzw. ausgefallene Redundanz, sofern zutreffend. Zum Beispiel: Der ursprüngliche Stromversorgungsmodus war beim Einschalten aller Blades „Power Supply Redundant“ (Netzteilredundant) (N+1) und wurde dann auf „AC Redundant“ (Wechselstromredundant) (N+N) geändert. In diesem Fall stellt sich dem Onboard Administrator eine reduzierte Stromkapazität dar. Solange genug Strom verfügbar ist, bleiben alle Blades in Betrieb. Unter bestimmten Umständen wird ein Blade, z. B. wenn er einen anderen Server Blade ersetzt, jedoch nicht eingeschaltet. Weitere Informationen finden Sie in der nachstehenden Tabelle und in den sich daran anschließenden Abschnitten.

Dynamic Power (Dynamische Stromversorgung): Die Standardeinstellung ist „Disabled“ (Deaktiviert). Die folgenden Optionen können ausgewählt werden:

- Enabled (Aktiviert): Einige Netzteile können automatisch in den Standby-Betrieb geschaltet werden, um die Gesamteffizienz des Stromversorgungs-Subsystems des Gehäuses zu steigern.
- Disabled (Deaktiviert): Alle Netzteile teilen die Last. Die Effizienz des Stromversorgungssubsystems ist je nach Last unterschiedlich.

HINWEIS: Die Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus) wird bei allen c3000-Netzteilen unterstützt. Sie wird bei allen c7000-Netzteilen außer solchen unterstützt, die mit niedriger Eingangsspannung (Nennwert 100-120 VAC) betrieben werden.

HINWEIS: Bei OA v4.01 und höher wurde der werksseitig eingestellte Standardwert, der mit der Einstellung „Dynamic Power“ (Dynamischer Stromsparmodus) verknüpft ist, aktiviert. Die Betriebseffizienz der derzeit verfügbaren HP Gold (92%ige Effizienz) und HP Platinum (94%ige Effizienz) Gehäuse-Netzteile macht diese firmwarebasierte Stromverwaltungsstrategie überflüssig. Die Einstellung für „Dynamic Power“ (Dynamischer Stromsparmodus) wird nur für HP Gehäuse-Netzteile mit einem Effizienzwert von weniger als 92 % empfohlen. Bei der Aktualisierung auf OA v4.01 oder höher wird die aktuelle Einstellung für „Dynamic Power“ (Dynamischer Stromsparmodus) nach der Aktualisierung beibehalten. Weitere Informationen finden Sie im Kundenratschlag c03957955 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03957955).

Power Limit (Strombegrenzung)

Legen Sie für ein leeres Gehäuse keinen Wert für „Static Power Limit“ (Statische Strombegrenzung) oder „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) fest.

Modus	Insight Display-Name	Beschreibung
Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)	Keine	Eine optionale Funktion, mit der Sie eine Stromobergrenze für eine Gruppe von Servern in einem Gehäuse festlegen können. Wenn die Server ausgeführt werden, ändert sich der Strombedarf für jeden Server. Für jeden Server wird die Stromobergrenze automatisch angepasst, um den Server mit genug Strom zu versorgen, damit er seine Arbeitsauslastungsanforderungen erfüllen kann, während er gleichzeitig die dynamische Stromobergrenze des Gehäuses einhält. Es ist eine redundante Onboard Administrator-Platine erforderlich, um die Funktion „Dynamic Power Cap“ (Dynamische Stromobergrenze) einzurichten. Die Funktion wird mit drei Konfigurationsparametern aktiviert: • Dynamic Power Cap (Dynamische Stromobergrenze): Die durchschnittliche Stromversorgung überschreitet die dynamische Stromobergrenze insgesamt nicht. • Derated Circuit Capacity (Herabgesetzte Schaltkreis-Kapazität): Die durchschnittliche Stromleistung auf einem einzelnen Schaltkreis überschreitet nicht die herabgesetzte Schaltkreiskapazität. • Rated Circuit Capacity (Nennkapazität des Schaltkreises): Die Stromspitzenleistung auf einem einzelnen Schaltkreis überschreitet nicht die Nennkapazität des Schaltkreises. Wenn diese Parameter konfiguriert werden, muss der Wert für „Derated Circuit Capacity“ (Herabgesetzte Schaltkreiskapazität) mindestens so groß sein wie der Wert für „Dynamic Power Cap“ (Dynamische Stromobergrenze) und nicht größer als der Wert für „Rated Circuit Capacity“ (Nennkapazität des Schaltkreises). Mit der dynamischen Stromobergrenze wird der Stromverbrauch des Gehäuses infolge einer Kühlungsauflage eingeschränkt, die einen niedrigeren Wert als die herabgesetzte Schaltkreiskapazität vorschreibt. Mit der herabgesetzten Schaltkreiskapazität wird der durchschnittliche Stromverbrauch des Gehäuses auf einem Schaltkreis begrenzt. Mit der Nennkapazität des Schaltkreises wird der Spitzenstromverbrauch des Gehäuses auf einem Schaltkreis begrenzt. Wenn Sie die elektrische Last oder abgegebene Wärme eines Gehäuses begrenzen möchten, ist eine dynamische Stromobergrenze des Gehäuses (Enclosure Dynamic Power

Modus	Insight Display-Name	Beschreibung
		Cap) dafür besser geeignet als eine statische Strombegrenzung (Static Power Limit). Bei einer dynamischen Stromobergrenze können mehr Blades eingeschaltet werden als bei einer statischen Strombegrenzung. Eine komplette Liste der durch die Option „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) unterstützten BladeSystem Server Blades finden Sie auf der HP Website (http://www.hp.com/go/dpc).
Static Power Limit (Statische Strombegrenzung)	Power Limit (Strombegrenzung)	Eine optionale Einstellung zur Strombegrenzung. Jedes Mal, wenn Sie versuchen, eine Komponente einzuschalten, werden der gesamte Strombedarf der neuen Komponente sowie der bereits eingeschalteten Komponenten mit dieser statischen Strombegrenzung verglichen. Überschreitet der gesamte Strombedarf den Grenzwert, wird das Einschalten der neuen Komponente verhindert. Unter den folgenden Bedingungen ist eine statische Strombegrenzung besser geeignet: • Die Obergrenzen sollen nicht dynamisch für die Blades angepasst werden. • Sie ziehen es vor, einen Server Blade nicht einzuschalten, wenn ihm nicht die volle Stromversorgung zugewiesen werden kann (auch wenn er in der Regel weniger Strom verbraucht). • Mehr als 1/4 der Blades im Gehäuse erfüllen nicht die Hardware- oder Firmwareanforderungen für die dynamische Stromobergrenze des Gehäuses.
Keine	Keine	Der Stromverbrauch des Gehäuses wird nicht verwaltet oder begrenzt.

Erläuterung von „Power Capping“ (Stromobergrenze), „Dynamic Power Capping“ (Dynamische Stromobergrenze) und „Enclosure Power Capping“ (Dynamische Stromobergrenze des Gehäuses)

HP bietet drei Möglichkeiten, mit denen der Benutzer den Stromverbrauch des Servers einschränken kann. Bei allen drei Strombegrenzungsoptionen wird der Stromverbrauch auf ein bestimmtes Watt- oder BTU/Stunde-Ziel eingeschränkt. Diese drei Technologien sind „Power Capping“ (Stromobergrenze), „Dynamic Power Capping“ (Dynamische Stromobergrenze) und „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses).

Stromobergrenzen

HP führte diese Technologie mit iLO 2, Version 1.30 im Mai 2007 ein. Diese firmwarebasierte Technologie begrenzt den durchschnittlichen Stromverbrauch des Servers auf ein benutzerdefiniertes Watt- oder BTU/Stunde-Ziel. Da diese Technologie in der Firmware ausgeführt wird, kann der Stromverbrauch nicht schnell genug eingeschränkt werden, um den Schutz der Trennschalter auf PDU-Ebene zu gewährleisten. Mit „Power Capping“ (Stromobergrenze) wird der Stromverbrauch für den Schutz der Kühlungsinfrastruktur schnell genug eingeschränkt. Daher ist dies eine wirksame Lösung für Datenzentren, deren Kühlungskapazität eingeschränkt ist. „Power Capping“ (Stromobergrenze) wird auf jedem ProLiant-Server oder -Blade unterstützt, der über einen iLO-Managementprozessor oder über Strommessfähigkeiten verfügt. Zur Verwendung von „Power Capping“ (Stromobergrenze) sind als Firmware iLO 2, Version 1.30 (oder höher) und ein aktualisiertes System-ROM/-BIOS erforderlich.

Dynamic Power Capping

„Dynamic Power Capping“ (Dynamische Stromobergrenze) ist eine hardwarebasierte Technologie, die den Stromverbrauch zum Schutz der Trennschalter und der Kühlungsinfrastruktur schnell genug einschränkt. HP führte „Dynamic Power Capping“ (Dynamische Stromobergrenze) mit iLO 2, Version 1.70 im Dezember 2008 ein. Unterstützte Server enthalten einen internen Hardwareschaltkreis, der den Server-Stromverbrauch auf sub-sekündiger Basis überwacht. Nähert sich der Server-Stromverbrauch der in iLO festgelegten Stromobergrenze, schränkt der interne Hardwareschaltkreis den Stromverbrauch schnell genug ein, um Schaltkreise auf PDU-Ebene vor einer Überzeichnung zu schützen und strombezogene Serverausfälle zu verhindern.

Für „Dynamic Power Capping“ (Dynamische Stromobergrenze) wird bestimmte Hardware auf der Systemplatine benötigt. „Dynamic Power Capping“ (Dynamische Stromobergrenze) erfordert ebenfalls als Firmware iLO 2, Version 1.70 (oder höher) und ein ROM/BIOS mit Datum vom 1.10.2008 (oder später). iLO aktualisiert Firmware im Hardwareschaltkreis für „Dynamic Power Capping“ (Dynamische Stromobergrenze) automatisch.

„Dynamic Power Capping“ (Dynamische Festlegung einer Stromobergrenze) wird auf den folgenden BladeSystem Server Blades unterstützt:

- BL260c G5 (Hinweise: 2)
- BL2x220 G5 (Hinweise: 2)
- BL460c G1 (Hinweise: 1 und 2)
- BL460c G5 (Hinweise: 2)
- BL465c G5 (Hinweise: 2)
- BL495c G5 (Hinweise: 2)
- BL685c G5 (Hinweise: 2)
- Alle G6 Server Blades
- Alle G7 Server Blades
- Alle G8 Server Blades

Weitere Informationen

- Zur Unterstützung der dynamischen Festlegung einer Stromobergrenze benötigen diese Systeme Quad-Core-fähige Systemplatinen.
- Wenn eine Stromobergrenze für das HP BladeSystem implementiert werden soll, empfiehlt HP die über den Onboard Administrator vorgenommene Einstellung „Enclosure Dynamic Power Capping “ (Dynamische Festlegung einer Stromobergrenze für das Gehäuse) zu wählen. Um die Funktion „Enclosure Dynamic Power Capping “ (Dynamische Festlegung einer Stromobergrenze für das Gehäuse) verwenden zu können, muss die iLO 2 Firmware auf Version 1.70 oder höher aktualisiert werden und empfiehlt es sich, das System-ROM auf Version 10/1/2008 oder höher zu aktualisieren. Bei einigen älteren BL460c Servern kann die iLO-Firmware den Hardwareschaltkreis für die Funktion „Dynamic Power Capping“ (Dynamische Stromobergrenze) möglicherweise nicht automatisch aktualisieren. In diesen Fällen kompensiert Onboard Administrator für den fehlenden internen Hardwareschaltkreis und garantiert weiterhin den Schaltkreisschutz.

Gehäusedynamische Stromobergrenzen

„Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) kombiniert die Stromobergrenzen-Technologie des BladeSystem Servers mit einem Stromausgleichs-Steueralgorithmus im Onboard Administrator-Modul, um die Gesamtleistung des Gehäuses zu

maximieren. „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) schützt die Trennschalter und optimiert die Leistung.

Mit „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) legen Sie eine Stromobergrenze für das gesamte Gehäuse fest. Das Onboard Administrator-Modul weist die einzelnen Grenzwerte automatisch jedem teilnehmenden Server Blade zu. Die Server Blades halten sich bei der Verwaltung an diesen Grenzwert. Das Onboard Administrator-Modul überwacht die Stromverbrauchsanforderungen für jeden Server Blade fortlaufend und gleicht die einzelnen Grenzwerte fortlaufend aus, um sicherzustellen, dass beanspruchte Server Blades mehr Strom erhalten als ruhende Server Blades. Durch diese Stromzuweisung wird die Gesamtleistung des Gehäuses verbessert.

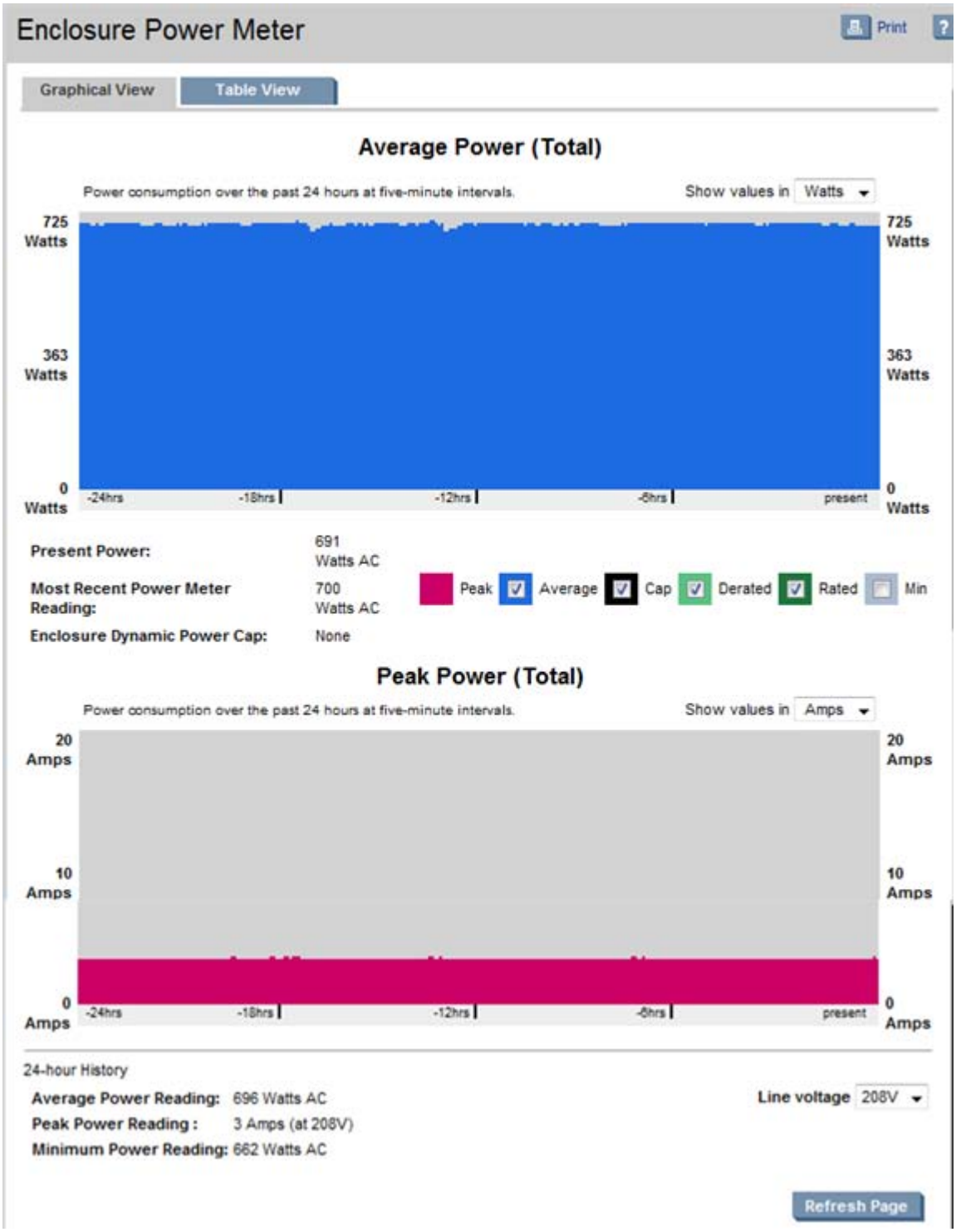
Die Stromobergrenzen für BladeSystem-Server werden im Onboard Administrator-Modul festgelegt. „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) schützt die Kühlungs- und elektrischen Infrastrukturen. „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) arbeitet mit firmwarebasierter Stromobergrenzen-Technologie auf dem Server oder mit der schnellen, hardwarebasierten Technologie. „Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) funktioniert besser, wenn die Server Blades, die die schnelle hardwarebasierte Obergrenzen-Technologie unterstützen, entsprechend aufgerüstet werden.

„Enclosure Dynamic Power Capping“ (Dynamische Stromobergrenze des Gehäuses) erfordert Onboard Administrator 2.30 (oder höher), iLO 2, Version 1.70 (oder höher) und System-ROM/BIOS ab dem 1.10.2008.

HINWEIS: Stromobergrenzen, die sich auf weniger als 50 % der Differenz zwischen maximaler Stromversorgung und Leerlauf-Stromversorgung belaufen, können aufgrund von Änderungen im Server möglicherweise nicht erreicht werden. Stromobergrenzen von weniger als 20 % werden nicht empfohlen und können bewirken, dass der Server neu gestartet wird oder das Server-Betriebssystem nicht mehr reagiert.

Bildschirm „Enclosure Power Meter“ (Gehäuse-Strommesser)

Der Bildschirm „Enclosure Power Meter“ (Gehäuse-Strommesser) zeigt den Spitzenstromverbrauch, den durchschnittlichen Stromverbrauch und die verfügbare zugewiesene Stromversorgung in einer Kurve an, anhand der sich die Stromversorgungssituation des Gehäuse schnell und leicht deuten lässt. Der Strommesser ist zum Aufzeigen von Trends im Stromverbrauch hilfreich und kann die Fehlerbeseitigung des Stromversorgungs-Subsystems erleichtern.



Registerkarte „Graphical View“ (Grafische Ansicht)

In diesem Bildschirm können Sie eine grafische Ansicht der Strommesswerte des Gehäuses einsehen.

Um zwischen Watt, BTU/Stunde und A umzuschalten, klicken Sie auf **Show Values** (Werte anzeigen).

Der Wert **Line Voltage** (Leitungsspannung) wird zur Konvertierung in Ampere verwendet. Der Standardwert basiert auf dem Netzteil-Hardwaremodell, nicht auf der tatsächlichen Netzspannung. Wählen Sie die tatsächliche Netzspannung für das Gehäuse für eine genauere Ampere-Konvertierung aus.

Um die aktualisierten Strommesswertinformationen anzuzeigen, klicken Sie auf **Refresh Page** (Seite aktualisieren).

Messwertkurve für durchschnittlichen Stromverbrauch

Dieses Diagramm zeigt den Stromverbrauch des Gehäuses während der letzten 24 Stunden. Onboard Administrator sammelt alle 5 Minuten Informationen zum Stromverbrauch und zur dynamischen Stromobergrenze des Gehäuses. Für jeden fünfminütigen Zeitraum werden der Spitzenverbrauch und der Durchschnittsverbrauch in einem Kreispuffer gespeichert. Diese Werte werden in Form eines Balkendiagramms angezeigt, wobei der Durchschnittswert blau, der Spitzenwert rot und der Grenzwert schwarz dargestellt werden. Diese Daten werden bei einem Gehäuse-Reset ebenfalls zurückgesetzt. Sie können festlegen, welche Informationen im Balkendiagramm angezeigt werden, indem Sie die Kontrollkästchen **Average, Cap, Derated, Rated** (Durchschnittswert, Obergrenze, Herabgesetzter Wert, Nennwert) und **Min** (Mindestwert) aktivieren bzw. deaktivieren.

Present Power (Aktueller Verbrauch)

Dieser Wert stellt die Leistung in Watt dar, die von allen Komponenten im Gehäuse verbraucht wird.

Most Recent Power Meter Reading (Letzter Strommesswert)

Dieser Wert stellt den neuesten Strommesswert des Gehäuses dar.

Messwertkurve des Spitzenverbrauchs

Dieses Diagramm zeigt den Spitzenstromverbrauch und die dynamische Stromobergrenze des Gehäuses während der vergangenen 24 Stunden an.

Die Anzeige „Peak Power“ (Spitzenstrom) wird zu „Peak Power (Side A + Side B)“ (Spitzenstrom (Seite A + Seite B)), wenn eine N+N redundante Stromversorgung vorhanden ist, und gibt an, dass der Spitzenwert auf zwei Stromkreise verteilt wird. Es werden außerdem zwei Kurven angezeigt: eine für Seite A und eine für Seite B.

Die Stromverteilung zwischen Seite A und Seite B wird anhand der Anzahl der aktiven Netzteile auf jeder Seite geschätzt. Bei Verlust der Redundanz zeigt die verloren gegangene Seite für den Spitzenstrom den Wert Null an.

Enclosure Dynamic Power Cap (Dynamische Stromobergrenze des Gehäuses)

Dieser Wert stellt die dynamische Stromobergrenze des Gehäuses dar.

Average Power Reading (Durchschnittlicher Strommesswert)

Dieser Wert stellt den Durchschnitt der Strommesswerte des Gehäuses in den vergangenen 24 Stunden dar. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Durchschnitt aller Messungen seit dem Einschalten des Gehäuses.

Peak Power Reading (Spitzenstrommesswert)

Dieser Wert stellt den Messwert für den Spitzenstrom des Gehäuses in den vergangenen 24 Stunden dar. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen seit dem Einschalten des Gehäuses oder dem Zurücksetzen von Onboard Administrator.

Die Anzeige „Peak Power“ (Spitzenstrom) wird zu „Peak Power (Side A + Side B)“ (Spitzenstrom (Seite A + Seite B)), wenn eine N+N redundante Stromversorgung vorhanden ist, und gibt an, dass der Spitzenwert auf zwei Stromkreise verteilt wird.

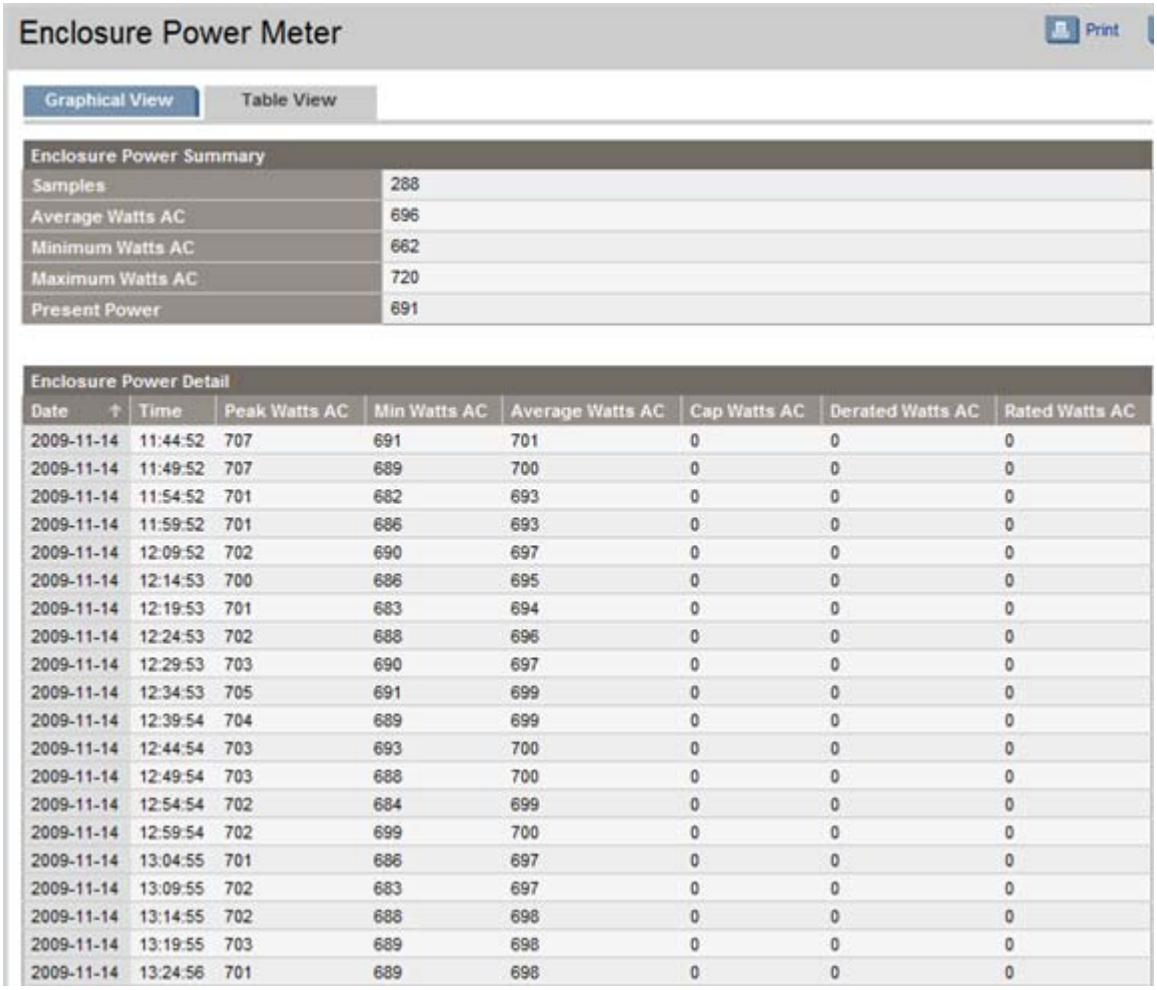
Minimum Power Reading (Minimaler Strommesswert)

Dieser Wert stellt den Messwert für den Mindeststrom des Gehäuses in den vergangenen 24 Stunden dar. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Mindestwert aller Messungen seit dem Einschalten des Gehäuses.

Refresh Page (Seite aktualisieren)

Wenn Sie ein Gehäuse neu starten, empfiehlt HP, fünf Minuten zu warten und dann auf **Refresh Page** (Seite aktualisieren) zu klicken, da der Strommesser nicht dynamisch aktualisiert wird.

Registerkarte „Table View“ (Tabellenansicht)



In diesem Bildschirm können Sie die Strommesswerte des Gehäuses im Tabellenformat einsehen.

Enclosure Power Summary (Gehäusestromversorgung – Zusammenfassung)

Zeile	Beschreibung
Samples (Messungen)	Anzahl der erfassten Messungen.
Average (Durchschnittswert) (Watt, BTU/Stunde oder Ampere)	Dieser Wert zeigt den Durchschnittswert der Strommesswerte (je nach Auswahl Watt, BTU/Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Durchschnitt aller Messungen, seit das Gehäuse eingeschaltet wurde.

Zeile	Beschreibung
Minimum (Mindestwert) (Watt, BTU/ Stunde oder Ampere)	Dieser Wert zeigt den Mindestwert der Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Mindestwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Maximum (Höchstwert) (Watt, BTU/ Stunde oder Ampere) (Side A + Side B) (Seite A + Seite B)	Dieser Wert zeigt den Höchstwert der Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Present Power (Aktueller Verbrauch)	Dieser Wert zeigt den Strom an, der von allen Komponenten im Gehäuse verbraucht wird.

Enclosure Power Detail (Detaillierte Strommesswerte des Gehäuses)

Die Tabelle „Enclosure Power Detail“ (Detaillierte Strommesswerte des Gehäuses) enthält detaillierte Informationen zu den einzelnen fünfminütigen Messungszeiträumen. Durch Klicken auf **Date** (Datum) im Tabellenkopf können Sie die Reihenfolge der detaillierten Strommesswerte des Gehäuses vom aktuellen Datum zum ältesten Datum oder umgekehrt anordnen.

Spalte	Beschreibung
Date (Datum)	Datum, an dem der Strommesswert ermittelt wurde.
Time (Uhrzeit)	Uhrzeit, zu der der Strommesswert ermittelt wurde.
Peak (Spitzenwert) (Watt, BTU/ Stunde oder Ampere) (Side A + Side B) (Seite A + Seite B)	Dieser Wert zeigt den Höchstwert der Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Min (Mindestwert) (Watt, BTU/ Stunde oder Ampere)	Dieser Wert zeigt den Mindestwert der Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Mindestwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Average (Durchschnittswert) (Watt, BTU/Stunde oder Ampere)	Dieser Wert zeigt den Durchschnittswert der Strommesswerte (je nach Auswahl Watt, BTU/Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Durchschnitt aller Messungen, seit das Gehäuse eingeschaltet wurde.
Cap (Höchstwert) (Watt, BTU/ Stunde oder Ampere)	Dieser Wert zeigt den maximalen dynamischen Stromobergrenzen-Messwert (je nach Auswahl Watt, BTU/Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Derated (Herabgesetzt) (Watt, BTU/ Stunde oder Ampere)	Dieser Wert zeigt die herabgesetzten Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen, seit das Gehäuse eingeschaltet wurde.
Rated (Nennwert) (Watt, BTU/ Stunde oder Ampere)	Dieser Wert zeigt den Nennwert der Strommesswerte (je nach Auswahl Watt, BTU/ Stunde oder Ampere) für das Gehäuse während der letzten 24 Stunden an. War das Gehäuse nicht 24 Stunden lang eingeschaltet, entspricht der Wert dem Höchstwert aller Messungen, seit das Gehäuse eingeschaltet wurde.

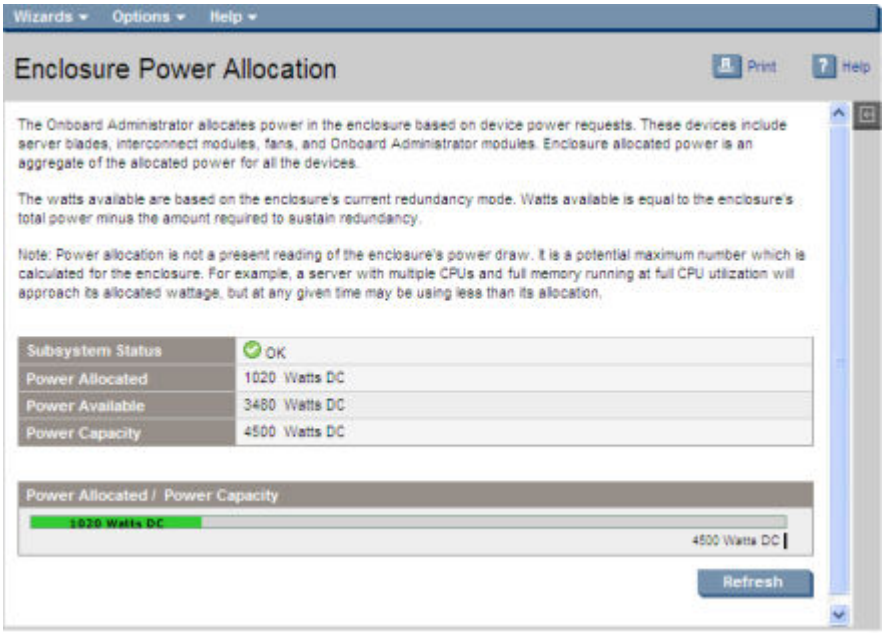
Power units (Stromversorgungseinheiten)

Wählen Sie aus dem Menü den Wert aus, in dem die Stromversorgungsdaten angezeigt werden sollen.

Line voltage (Leitungsspannung)

Wählen Sie aus dem Menü die Leitungsspannung aus.

Gehäusestromzuordnung


Wizards
Options
Help
Enclosure Power Allocation
Print
Help
The Onboard Administrator allocates power in the enclosure based on device power requests. These devices include server blades, interconnect modules, fans, and Onboard Administrator modules. Enclosure allocated power is an aggregate of the allocated power for all the devices.
The watts available are based on the enclosure's current redundancy mode. Watts available is equal to the enclosure's total power minus the amount required to sustain redundancy.
Note: Power allocation is not a present reading of the enclosure's power draw. It is a potential maximum number which is calculated for the enclosure. For example, a server with multiple CPUs and full memory running at full CPU utilization will approach its allocated wattage, but at any given time may be using less than its allocation.
Subsystem Status
OK
Power Allocated
1020 Watts DC
Power Available
3480 Watts DC
Power Capacity
4500 Watts DC
Power Allocated / Power Capacity
1020 Watts DC
4500 Watts DC
Refresh

Im Bildschirm „Power Allocation“ (Stromzuordnung) werden Basisinformationen zur Gesamtkapazität des Stromversorgungs-Subsystems, zur redundanten Kapazität und zur zugewiesenen Leistung in Watt angezeigt. Die Grafik „Enclosure Internal Power“ (Gehäuse – Interner Strom) zeigt die zugeordnete Wattzahl in grüner Farbe auf einem grauen Hintergrund, der die gesamte redundante Kapazität der Stromversorgungen repräsentiert.

Wenn Sie den Gehäuse-Redundanzmodus ändern, nachdem den Geräten bereits Strom zugewiesen wurde, wird das Stromversorgungs-Subsystem dadurch möglicherweise beeinträchtigt. Die Geräte werden weiterhin mit Strom versorgt, die Redundanz funktioniert möglicherweise aber nicht richtig. Wenn null Watt verfügbar sind und ein beeinträchtigtes Stromdiagramm angezeigt wird, überprüfen Sie Ihr Stromversorgungs-Subsystem und Ihre Redundanz-Konfigurationen. Sie können die Beeinträchtigung durch Ändern des Redundanzmodus oder durch Hinzufügen weiterer Netzteile zum Gehäuse beheben.

Bei Redundanzverlust entspricht die „Power Capacity“ (Stromkapazität) dem Wert von „Power Allocated“ (Zugewiesener Strom).

Enclosure Power Summary (Gehäusestromversorgung – Zusammenfassung)

Enclosure Input Power Summary (Eingangsstrom des Gehäuses – Zusammenfassung)

„Present Power“ (Aktueller Strom) entspricht den Eingangs-Watt zum Gehäuse und wird in Watt Wechselstrom bei Netzteilen mit AC-Eingabe und in Watt Gleichstrom bei Netzteilen mit DC-Eingabe gemessen. „Max Input Power“ (Max. Eingangsstrom) entspricht den höchsten erwarteten Eingangs-Watt. Ist ein Wert für „Power Limit“ (Strombegrenzung) festgelegt, entspricht der Wert für „Max Input

Power“ (Max. Eingangsstrom) dem Wert für „Power Limit“ (Strombegrenzung). Ist ein Wert für „Enclosure Dynamic Power Cap“ (Stromobergrenze des Gehäuses) festgelegt und EDPC aktiviert, dann entspricht der Wert für „Max Input Power“ (Max. Eingangsstrom) dem Wert für „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses). Ist weder ein Wert für „Enclosure Dynamic Power Cap“ (Stromobergrenze des Gehäuses) noch für „Power Limit“ (Strombegrenzung) festgelegt, dann entspricht der Wert für „Max Input Power“ (Max. Eingangsstrom) des Gehäuses dem erwarteten Eingangsstrom für das Gehäuse zur Inbetriebnahme bei maximaler Gleichstrom-Ausgabekapazität.

Enclosure Output Power Summary (Ausgangsstrom des Gehäuses – Zusammenfassung)

Wenn EDPC deaktiviert ist, basiert der Wert für „Power Capacity“ (Stromkapazität) auf der Anzahl der installierten und betriebsfähigen Netzteile, deren Gleichstrom-Ausgabekapazitäten und der redundanten Einstellung für „Power Mode“ (Stromversorgungsmodus). Der Wert für „Power Allocated“ (Zugewiesener Strom) ist die Gesamtstromausgabe des Gehäuses, die für Geräteeinschübe, Verbindungsmoduleinschübe und Lüfter zugewiesen wird. Der Wert für „Power Available“ (Verfügbarer Strom) entspricht dem Wert für „Power Capacity“ (Stromkapazität) minus des Wertes für „Power Allocated“ (Zugewiesener Strom).

Wenn EDPC aktiviert ist, entspricht die „Power Capacity“ (Stromkapazität) der „Enclosure Dynamic Power Cap“ (Dynamische Stromobergrenze des Gehäuses) in Watt Gleichstrom. „Power Allocated“ (Zugewiesener Strom) ist der Mindeststrom, auf den das Gehäuse begrenzt werden kann, in Watt Gleichstrom. Der Wert für „Power Available“ (Verfügbarer Strom) entspricht dem Wert für „Power Capacity“ (Stromkapazität) minus des Wertes für „Power Allocated“ (Zugewiesener Strom).
Der insgesamt für Geräteeinschübe, Verbindungsmoduleinschübe und Lüfter zugewiesene Strom entspricht möglicherweise nicht dem Wert für „Power Allocated“ (Zugewiesener Strom) für das Gehäuse, da die Stromobergrenze eines jeden Servers dynamisch gesteuert wird.

Enclosure Bay Output Power Allocation (Ausgangsstromzuweisung an Komponenteneinschübe)

Der Wert für „Power Allocated“ (Zugewiesener Strom) ist der allen Geräteeinschüben, Verbindungsmoduleinschüben und Lüftern insgesamt zugeordnete Strom.

Device Bay Power Summary (Geräteeinschubs-Stromversorgung – Zusammenfassung)

Jeder bestückte Geräteeinschub wird mit dem zugewiesenen Strom aufgeführt. Wenn EDPC aktiviert ist, zeigen zusätzliche Spalten Stromobergrenze (Power Cap), Prozentsatz der Stromobergrenze (% Power Cap) und den aktuelle Verbrauch (Present Power) kompatibler ProLiant-Server an.
Die Stromobergrenze in Prozent (% Power Cap) wird basierend auf der aktuellen Stromobergrenze in Watt (Power Caps Watts) dividiert durch den zugewiesenen Strom in Watt (Power Allocated Watts) berechnet. Wenn EDPC aktiviert ist, wird es einem Strom anfordernden Server Blade nur gestattet sich einzuschalten, wenn der Wert für „Power Available“ (Verfügbarer Strom) die Anforderung unterstützt oder das Onboard Administrator-Modul die Stromobergrenze für andere Server ändern kann, die die Anforderung unterstützen.

Interconnect Bay Power Summary (Stromversorgung der Verbindungsmoduleinschübe - Zusammenfassung)

Aufgeführt werden die einzelnen bestückten Verbindungsmoduleinschübe mit dem jeweils zugewiesenen Strom.

Fan Power Summary (Lüfter-Stromversorgung – Zusammenfassung)

Lüfter-Strom wird basierend auf einer Lüfterregel zugewiesen. Die Lüfterregel wird anhand des Gehäusetyps (c3000 oder c7000) und der belegen Geräteeinschübe bestimmt. Aufgelistet werden die Stromzuweisung an die Lüfter und der aktuelle Gesamtstromverbrauch aller Lüfter.

Um die Zusammenfassung der Stromversorgung zu aktualisieren, klicken Sie auf **Refresh** (Aktualisieren).

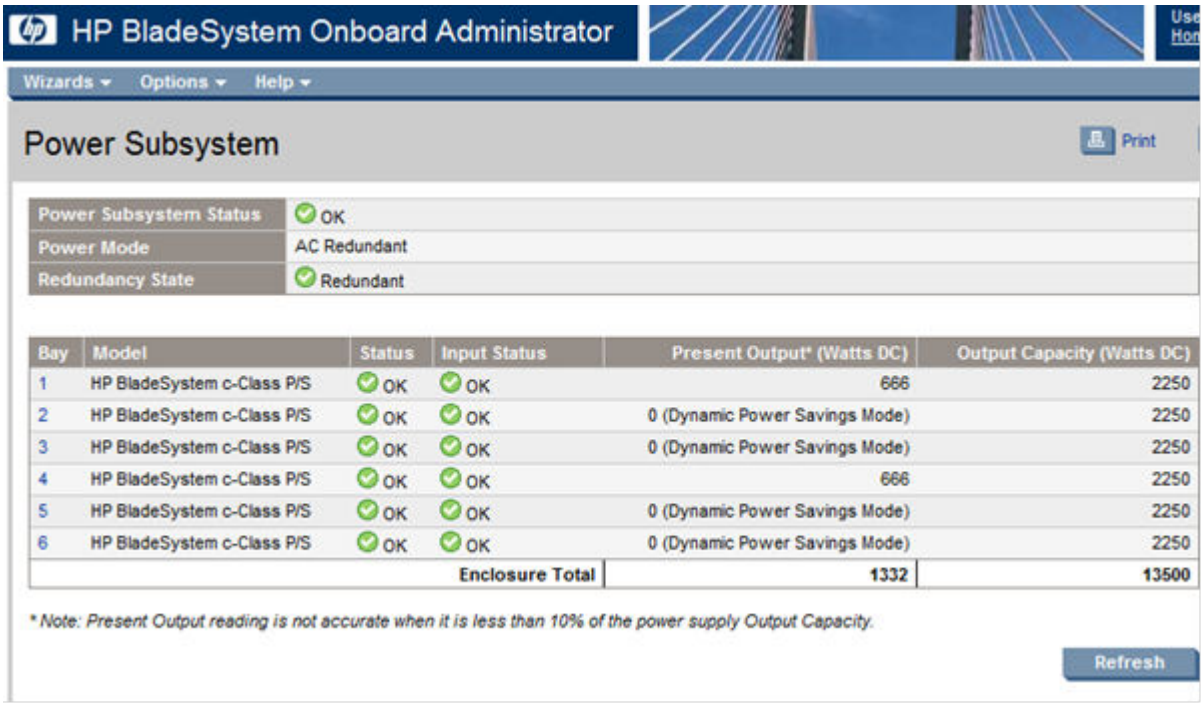
Bildschirm „Power Subsystem“ (Stromversorgungs-Subsystem)

Netzteile, die zur Verwendung in BladeSystem-Gehäusen verfügbar sind

Alle Netzteile in einem Gehäuse müssen die gleiche Teilenummer haben. Onboard Administrator weist mit einem entsprechenden Symbol darauf hin, welche Netzteile ersetzt werden müssen.

Power Supply Summary (Übersicht über Netzteile)

Der Bildschirm „Power Subsystem“ (Stromversorgungs--Subsystem) zeigt den Status des Stromversorgungs-Subsystems und einzelner Netzteile sowie Fehlerbedingungen an.


HP BladeSystem Onboard Administrator
Wizards
Options
Help
Power Subsystem
Print
Power Subsystem Status
OK
Power Mode
AC Redundant
Redundancy State
Redundant
Bay
Model
Status
Input Status
Present Output* (Watts DC)
Output Capacity (Watts DC)
1 HP BladeSystem c-Class P/S OK OK 666 2250
2 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
3 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
4 HP BladeSystem c-Class P/S OK OK 666 2250
5 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
6 HP BladeSystem c-Class P/S OK OK 0 (Dynamic Power Savings Mode) 2250
Enclosure Total 1332 13500
* Note: Present Output reading is not accurate when it is less than 10% of the power supply Output Capacity.
Refresh

Dieser Bildschirm enthält Informationen zum Status des Stromversorgungs-Subsystems und zu den einzelnen Netzteilen.

Power Subsystem (Stromversorgungs-Subsystem)

Zeile	Beschreibung
Power Subsystem Status (Status des Stromversorgungs-Subsystems)	Der Status des Stromversorgungs-Subsystems. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Power Mode (Stromversorgungsmodus)	Eine Benutzereinstellung zur Konfiguration der Gleichstromkapazität des Gehäuses und der Redundanz der Stromzufuhr des Gehäuses. Mögliche Werte sind „Redundant“, „AC Redundant“ (Netzredundant), „Power Supply Redundant“ (Netzteilredundant), „Not Redundant“ (Nicht redundant) oder „Unkown“ (Unbekannt).
Redundancy State (Redundanzstatus)	Gibt den Redundanzstatus des Stromversorgungs-Subsystems an. Mögliche Werte sind: Redundant, Not Redundant (Nicht redundant), Redundancy Lost (Verlust der Redundanz).

Netzteilstatus

Spalte	Beschreibung
Bay (Einschub)	Der Einschub innerhalb des Gehäuses des entsprechenden Netzteils. Dieses Feld zeigt nur bestückte Einschübe an. Leere Einschübe erscheinen nicht in dieser Tabelle.
Model (Modell)	Die Modellbezeichnung des Netzteils.
Status (Zustand)	Der allgemeine Status der Netzteils. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Input Status (Status der Eingangsleistung)	Der Status der Eingangsleistung des Netzteils. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Present Output (Watts) (Aktuelle Ausgangsleistung (Watt))	Dieser Wert ist ein Maß der aktuellen Ausgangsleistung des Netzteils in Watt.
Output Capacity (Watts) (Ausgangsleistung (Watt))	Die Menge der vom Netzteil abgegebenen Stromleistung in Watt. Dies ist ein Maß der vom Netzteil abgegebenen Gleichstrom-Ausgangsleistung in Watt.

Klicken Sie auf **Refresh** (Aktualisieren), um die Angaben zum Stromversorgungs-Subsystem zu aktualisieren.

Netzteilinformationen

Bei Auswahl eines bestimmten Netzteils wird die Seite „Power Supply Information—Bay x“ (Netzteilinformationen – Einschub x) geöffnet, wobei „x“ der Einschub des ausgewählten Netzteils ist. Dieser Bildschirm enthält Statusinformationen zum ausgewählten Netzteil.

Statusinformationen

Zeile	Beschreibung
Status (Zustand)	Der allgemeine Status der Netzteils. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Input Status (Status der Eingangsleistung)	Der Status der Eingangsleistung des Netzteils. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Present Output (Aktuelle Ausgabe)	Die Menge der vom Netzteil abgegebenen Stromleistung im Wechsel- und Gleichstrommodus. Dieser Wert wird in Watt angegeben.
Output Capacity (Ausgabekapazität)	Die maximale Menge der Stromleistung, die das Netzteil im Wechsel- und Gleichstrommodus abgeben kann. Dieser Wert wird in Watt angegeben.
Model (Modell)	Die Modellbezeichnung des Netzteils.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Netzteils.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatznetzteils dieser Art zu verwendende Teilenummer.
Spare Part Number (Ersatzteilnummer)	Die bei der Bestellung eines zusätzlichen Netzteils oder eines Ersatznetzteils zu verwendende Ersatzteilnummer.

Diagnostic information (Diagnoseinformationen)

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Die überprüften Komponenten-Identifikationsdaten sind Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen. Diese Daten werden auch als FRU-Daten bezeichnet. Ein Komponenten-Identifikationsdaten-Fehler wird angezeigt, wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Location (Komponentenposition)	Inkorrekter Standort des Netzteils. Mögliche Werte sind „OK“ und „Incorrect location for proper device cooling“ (Inkorrekte Position für angemessene Komponentenkühlung).
Device Operational (Komponente betriebsbereit)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator nicht angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Degraded (Komponente beeinträchtigt)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator angefordert. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Power Cord (Netzkabel)	Eingangsstromstatus. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Mismatch (Unstimmige Komponente)	Dieses Feld gibt an, dass im gleichen Gehäuse unterschiedliche Netzteilmodelle installiert sind. In jedem Einschub müssen die gleichen Netzteilmodelle installiert sein.
Service Action (Servicemaßnahme)	Die zur Korrektur eines Netzteilfehlers empfohlene zu ergreifende Servicemaßnahme.

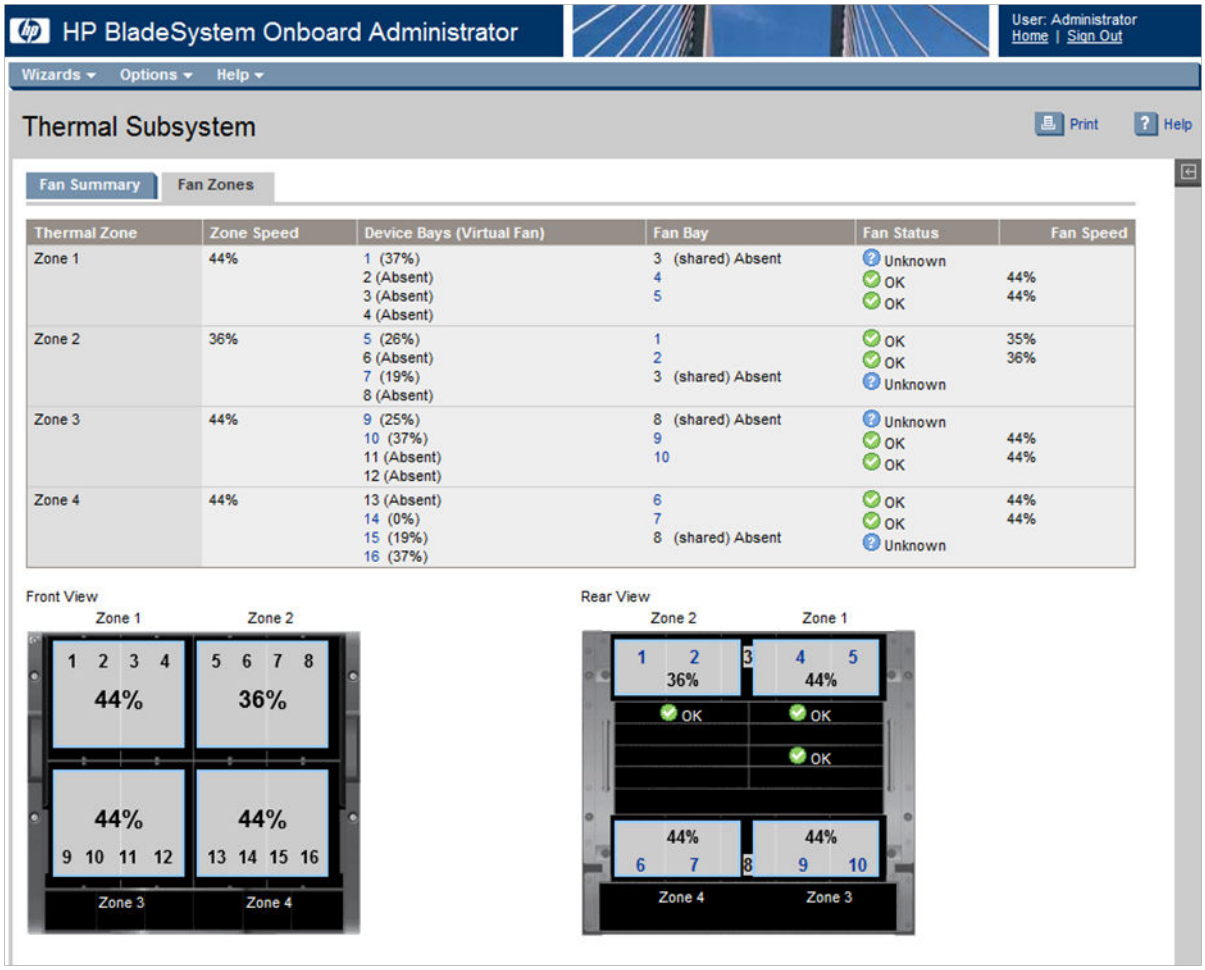
Klicken Sie auf **Refresh** (Aktualisieren), um die Angaben zum Stromversorgungs-Subsystem zu aktualisieren.

Management von Lüftern und Kühlung

Lüfterzonen

Lüfterzonen dienen zur Überwachung der Einschubskühlungseffizienz und des Status der Einschübe, für deren Kühlung die Lüfter konfiguriert sind. Die gemeldeten Zonengeschwindigkeiten sind Zielgeschwindigkeiten. Diese Werte ändern sich mit der Zeit, da die Lüftergeschwindigkeit je nach Kühlbedarf der jeweiligen Zone zu- bzw. abnimmt. Der Bildschirm „Lüfterzonen“ wird nicht dynamisch aktualisiert. Um die Informationen auf diesem Bildschirm zu aktualisieren, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Lüftergeschwindigkeiten werden als Prozentsatz der Gesamtkapazität angezeigt. Lüfter, die in einer Zone ohne Blades in Betrieb genommen werden, laufen mit einer minimalen Drehzahl von 30 %, um die ordnungsgemäße Kühlung des gesamten Gehäuses aufrechtzuerhalten.


HP BladeSystem Onboard Administrator
User: Administrator
Home | Sign Out
Wizards
Options
Help
Thermal Subsystem
Print
Help
Fan Summary
Fan Zones
Thermal Zone | Zone Speed | Device Bays (Virtual Fan) | Fan Bay | Fan Status | Fan Speed
Zone 1 | 44% | 1 (37%) 2 (Absent) 3 (Absent) 4 (Absent) | 3 (shared) Absent 4 5 | Unknown OK OK | 44% 44%
Zone 2 | 36% | 5 (26%) 6 (Absent) 7 (19%) 8 (Absent) | 1 2 3 (shared) Absent | OK OK Unknown | 35% 36%
Zone 3 | 44% | 9 (25%) 10 (37%) 11 (Absent) 12 (Absent) | 8 (shared) Absent 9 10 | Unknown OK OK | 44% 44%
Zone 4 | 44% | 13 (Absent) 14 (0%) 15 (19%) 16 (37%) | 6 7 8 (shared) Absent | OK OK Unknown | 44% 44%
Front View
Zone 1
Zone 2
1 2 3 4
44%
5 6 7 8
36%
44%
9 10 11 12
44%
13 14 15 16
Zone 3
Zone 4
Rear View
Zone 2
Zone 1
1 2
36%
3
4 5
44%
OK
OK
OK
44%
6 7
8
44%
9 10
Zone 4
Zone 3

Spalte	Beschreibung
Thermal Zone (Thermische Zone)	Die vier Kühlungszonen im Gehäuse: oben links, oben rechts, unten links und unten rechts.
Zone Speed (Zonengeschwindigkeit)	Die laut Berechnungen erforderliche Lüftergeschwindigkeit basierend auf dem höchsten Komponentenbedarf in der Zone.
Device Bays (Geräteeinschübe)	Die Anzahl der Geräteeinschübe in einer bestimmten thermischen Zone.
Fan Bay (Lüftereinschub)	Die Nummer des Lüftereinschubs. Die Lüfter in den Einschüben 3 und 8 befinden sich in mehr als einer thermischen Zone.
Fan Status (Lüfterstatus)	Der allgemeine Zustand jedes Lüfters. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt), „Failed“ (Fehler), „Absent“ (Nicht vorhanden).
Fan Speed (Lüftergeschwindigkeit)	Die Lüftergeschwindigkeit wird als Prozentsatz der maximalen Drehzahl angezeigt.

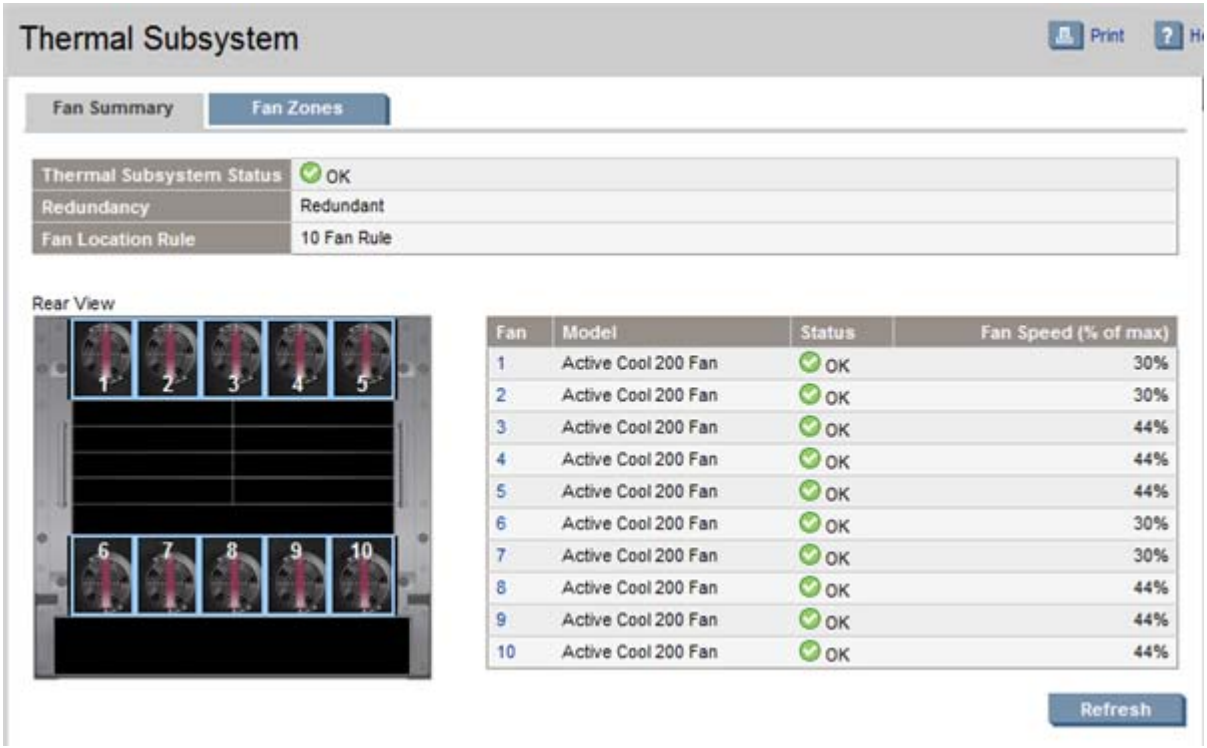
Thermal Subsystem (Thermisches Subsystem)

Onboard Administrator überwacht bis zu 10 Lüfter innerhalb des Gehäuses und reguliert die Lüftergeschwindigkeiten bei Bedarf basierend auf den Temperatur- und Strommessungen. Die Geschwindigkeit der einzelnen Lüfter lässt sich anpassen, um den Geräuschpegel und den Stromverbrauch zu reduzieren und um Luftstromunterschiede innerhalb des Gehäuses

auszugleichen. Die Leistung jedes Lüfters wird überwacht, und Onboard Administrator meldet dem Systemprotokoll und HP SIM (bei Aktivierung von SNMP) Fehler oder Warnungen.

Lüfterzonen können nur für das c7000-Gehäuse überwacht werden. Alle anderen Subsystemmerkmale und -funktionen sind bei den c3000- und c7000-Gehäusen identisch, sofern nicht anderweitig vermerkt.

Der folgende Bildschirm zeigt die Seite „Fan Summary“ (Lüfter – Zusammenfassung) für ein c7000-Gehäuse.



Fan Summary (Lüfter-Zusammenfassung)

Dieser Bildschirm enthält Informationen zum Status des thermischen Subsystems und zu den einzelnen Lüftern.

Lüftersubsystem, Status

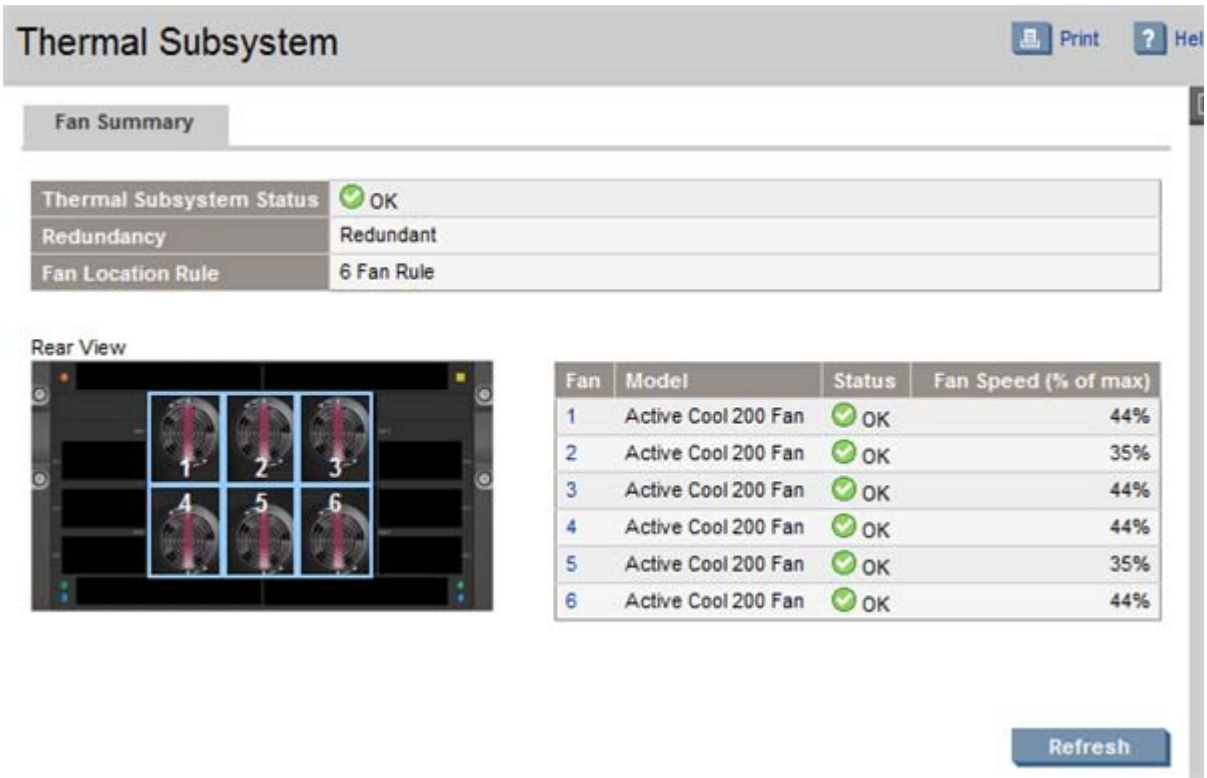
Zeile	Beschreibung
Thermal Subsystem Status (Status des thermischen Subsystems)	Gibt den allgemeinen Zustand des Lüftersubsystems an. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt) und „Critical Error“ (Kritischer Fehler).
Redundancy (Redundanz)	Gibt den Redundanzstatus der Lüfter an. Mögliche Werte sind: „Redundant“, „Nicht redundant“.
Fan Location Rule (Lüfterpositionsregel)	Diese Regel gibt die richtige Position der Lüfter und der unterstützten Geräteeinschübe an.

Lüfterstatus

Spalte	Beschreibung
Fan (Lüfter)	Der Einschub im Gehäuse des zugehörigen Lüfters.

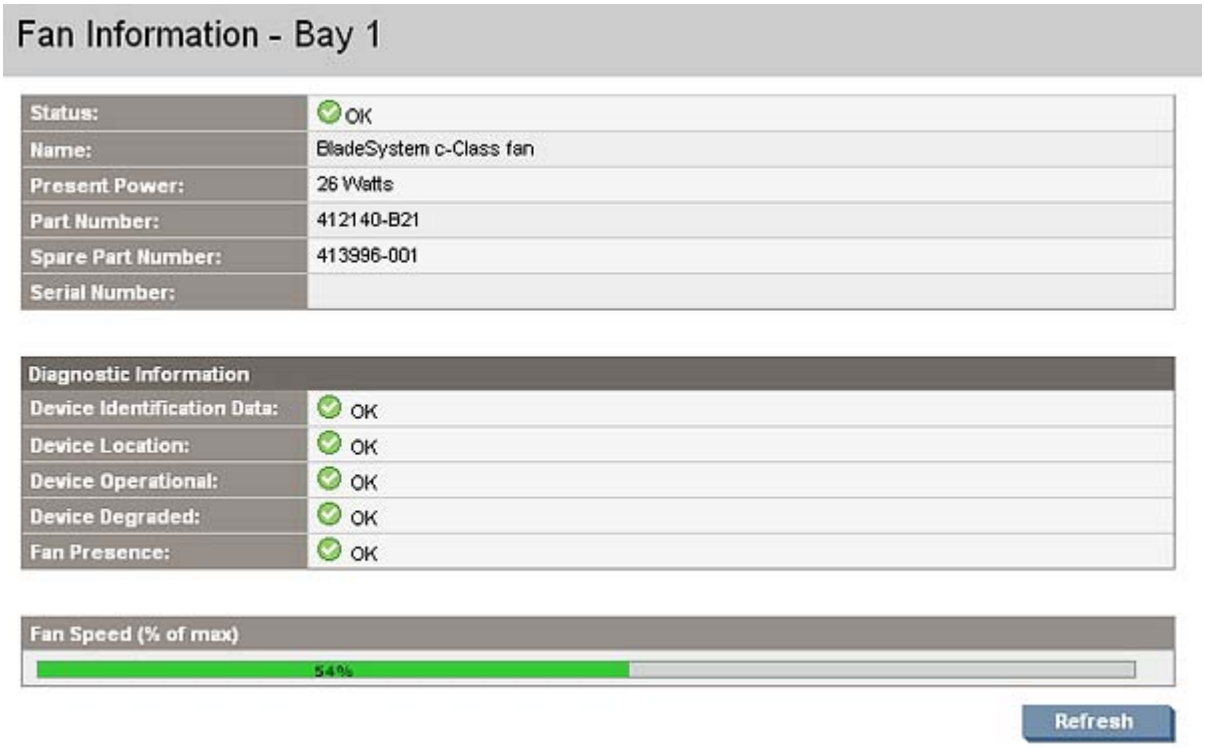
Spalte	Beschreibung
Model (Modell)	Die Modellbezeichnung des Lüfters.
Status (Zustand)	Gibt den allgemeinen Status des Lüfters an. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt), „Failed“ (Fehler), „Absent“ (Nicht vorhanden).
Fan Speed (Lüftergeschwindigkeit)	Die Lüftergeschwindigkeit wird als Prozentsatz der maximalen Drehzahl angezeigt.

Der folgende Bildschirm zeigt die Seite „Fan Summary“ (Lüfter – Zusammenfassung) für ein c3000-Gehäuse.

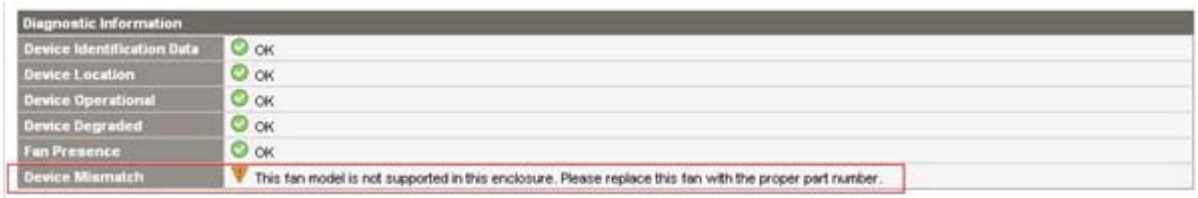


Sollte ein Lüftermodul ausfallen, kompensieren die verbleibenden Lüfter dies automatisch, indem sie die Lüftergeschwindigkeiten anpassen.

Sie können den Status eines jeden Lüfters einsehen, indem Sie den entsprechenden Lüfter entweder aus der Navigationsstruktur oder der grafischen Navigation auswählen. Der Bildschirm „Fan Information“ (Lüfterinformationen) enthält Informationen über den allgemeinen Zustand, den Namen, die Menge des Stromverbrauchs in Watt, die Ersatzteilnummer und die Seriennummer. Auf dem Bildschirm „Fan Information“ (Lüfterinformationen) werden außerdem Diagnoseinformationen zu internen Datenfehlern, Positionsfehlern, Komponentenausfällen, beeinträchtigten Komponenten und unstimmigen Komponenten angezeigt. Lüftergeschwindigkeiten werden in Umdrehungen/Minute (rpm) angezeigt. Um die Informationen auf dieser Seite zu aktualisieren, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).



Dieser Bildschirm zeigt einen Fehler aufgrund eines unstimmigen Lüfters an.


Diagnostic Information
Device Identification Data OK
Device Location OK
Device Operational OK
Device Degraded OK
Fan Presence OK
Device Mismatch This fan model is not supported in this enclosure. Please replace this fan with the proper part number.

Bei der Auswahl eines bestimmten Lüfters wird die Seite „Fan Information“ (Lüfterinformationen) für Einschub *x* geöffnet, wobei *x* der Einschub des ausgewählten Lüfters ist. Dieser Bildschirm enthält Statusinformationen zum ausgewählten Lüfter.

Statusinformationen

Zeile	Beschreibung
Status (Zustand)	Der allgemeine Status des Lüfters. Mögliche Werte sind „Unknown“ (Unbekannt), „OK“, „Degraded“ (Beeinträchtigt), „Failed“ (Fehler) und „Other“ (Sonstiges).
Name	Der allgemeine beschreibende Name des Lüfters.
Present Power (Aktueller Verbrauch)	Die vom Lüfter verbrauchte Strommenge.
Part Number (Artikelnummer)	Die bei der Bestellung eines zusätzlichen oder eines Ersatzlüfters dieser Art zu verwendende Teilenummer.
Spare Part Number (Ersatzteilnummer)	Die bei der Bestellung eines zusätzlichen Netzteils oder eines Ersatznetzteils zu verwendende Ersatzteilnummer.
Serial Number (Seriennummer)	Die eindeutige Seriennummer des Lüfters.

Diagnostic information (Diagnoseinformationen)

Diagnoseinformationen werden entweder durch Abfrage eines Komponenten-Mikrocontrollers gesammelt (was zu einem beeinträchtigten Status („Degraded“) führt, falls ein Fehler aufgetreten ist) oder vom Komponenten-Mikrocontroller ohne Abfrage gesendet, um einen Ausfall zu melden.

Zeile	Beschreibung
Device Identification Data (Komponenten-Identifikationsdaten)	Angaben wie Modellname, Teilenummer und Seriennummer sowie andere zur Identifikation der Komponenten verwendete Informationen werden überprüft. Diese Daten werden auch als FRU-Daten bezeichnet. Wenn die Daten nicht vorhanden sind oder nicht von Onboard Administrator gelesen werden können, wird ein Komponenten-Identifikationsdaten-Fehler angezeigt. Mögliche Werte sind „OK“ oder „Error“ (Fehler).
Device Location (Komponentenposition)	Inkorrekte Position des Lüfters. Mögliche Werte sind „OK“ und „Incorrect location for proper device cooling“ (Inkorrekte Position für angemessene Komponentenkühlung).
Device Operational (Komponente betriebsbereit)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator nicht angefordert.
Device Degraded (Komponente beeinträchtigt)	Die Komponente ist ausgefallen; der Status wurde von Onboard Administrator angefordert.
Fan Presence (Lüfterpräsenz)	Dieses Feld gibt an, ob zur Unterstützung der aktuellen Lüfterregel ein Lüfter benötigt wird.
Device Mismatch (Unstimmige Komponente)	Dieses Feld gibt an, dass im gleichen Gehäuse unterschiedliche Lüftermodelle installiert sind. In jedem Einschub müssen die gleichen Lüftermodelle installiert sein.

Lüftermodelle

Das c3000-Gehäuse unterstützt Active Cool 100- und Active Cool 200-Lüftermodelle. Das c7000-Gehäuse unterstützt nur das Active Cool 200-Lüftermodell. Im c3000-Gehäuse dürfen nicht gleichzeitig zwei verschiedene Lüftermodelle installiert werden. Wenn Sie Lüftermodelle miteinander vermischen oder ein falsches Lüftermodell im Gehäuse einbauen, wird in der Diagnose-Informationstabelle der Fehler **Device Mismatch** (Unstimmige Komponenten) angezeigt.

Um die Lüfter-Informationen zu aktualisieren, klicken Sie auf **Refresh** (Aktualisieren).

Informationen zur korrekten Installation der Lüfter im Gehäuse finden Sie im entsprechenden HP BladeSystem c7000-Gehäuse Setup- und Installationshandbuch.

Regeln zur Lüfterposition für das c7000-Gehäuse

Das HP BladeSystem c7000-Gehäuse wird mit mindestens vier HP Active Cool 200-Lüftern geliefert und unterstützt bis zu zehn Lüfter. Sie müssen die Lüfter in Gruppen mit geraden Zahlen basierend auf der Gesamtzahl der im Gehäuse installierten Server Blades installieren: Setzen Sie in allen nicht verwendeten Lüftereinschüben Lüfter-Blindmodule ein.

Regel für vier Lüfter

Lüftereinschübe 4, 5, 9 und 10 dienen zur Unterstützung von beliebigen unterstützten Kombinationen von Server Blades in maximal zwei Geräteeinschüben in den Geräteeinschüben 1, 2, 9 oder 10.

Regel für sechs Lüfter

Lüftereinschübe 3, 4, 5, 8, 9 und 10 dienen zur Unterstützung von beliebigen unterstützten Kombinationen von Server Blades in maximal acht Geräteeinschüben in den Geräteeinschüben 1, 2, 3, 4, 9, 10, 11 oder 12.

Regel für acht Lüfter

Lüftereinschübe 1, 2, 4, 5, 6, 7, 9 und 10 dienen zur Unterstützung von beliebigen unterstützen Kombinationen von Server Blades in allen Geräteeinschüben.

Regel für zehn Lüfter

Alle Lüftereinschübe dienen zur Unterstützung von beliebigen unterstützten Kombinationen von Server Blades in allen Geräteeinschüben.

Allgemeine Lüfterregeln

- Für ein Gehäuse, das mit einem Dreiphasen-Stromeingangsmodul konfiguriert ist, werden mindestens 6 Lüfter benötigt.
- Es werden mindestens 8 Lüfter benötigt, wenn mindestens ein Switchmodul in Verbindungseinschub 1, 3, 5 oder 7 und mindestens ein Switchmodul in Verbindungsmoduleinschub 2, 4, 6 oder 8 installiert ist. Dies gilt nicht für Passthrough-Module.
- Zehn Lüfter werden benötigt für eine Konfiguration mit:
  - einem oder mehreren HP Virtual Connect FlexFabric-20/40 F8-Modulen
  - einem oder mehreren D2220sb Speicher-Blades
  - mehr als der Hälfte der Gehäuse-Geräteeinschübe in belegtem Zustand und einer beliebigen Anzahl vorhandener D2200sb Speicher-Blades
  - neun oder mehr HP BL460c G1 und/oder HP BL460c G5 Server Blades

  HINWEIS: Zur Gewährleistung einer maximalen Kühlungseffizienz und Redundanz, reduziertem Stromverbrauch und reduziertem Geräuschpegel rät HP sehr zu zehn Lüftern für alle Konfigurationen.

Regeln zur Lüfterposition für das c3000-Gehäuse

Das HP BladeSystem c3000-Gehäuse wird mit vier HP Active Cool 100-Lüftern geliefert und unterstützt bis zu sechs Lüfter. Sie müssen die Lüfter in Gruppen mit geraden Zahlen basierend auf der Gesamtzahl der im Gehäuse installierten Server Blades installieren. Setzen Sie in allen nicht verwendeten Lüftereinschüben Lüfter-Blindmodule ein.

Regel für vier Lüfter

Für ein bis vier Speicher- oder Server Blades halber Höhe oder für ein bis zwei Speicher- oder Server Blades voller Höhe verwenden Sie die Lüftereinschübe 2, 4, 5 und 6 zur Unterstützung von maximal vier Geräteeinschüben in den Geräteeinschüben 1, 2, 5 oder 6.

Regel für sechs Lüfter

Für weitere Speicher- oder Server Blades installieren Sie sechs Lüfter unter Nutzung aller Geräteeinschübe.

HINWEIS: Im gleichen Gehäuse können nicht HP Active Cool 100 Lüfter zusammen mit HP Active Cool 200 Lüftern installiert werden. Onboard Administrator sendet eine Fehlermeldung, und Sie müssen die Art von Lüfter mit der geringeren Anzahl installierter Einheiten entfernen.

Verwalten von Benutzern

Users/Authentication (Benutzer/Authentifizierung)

In diesem Abschnitt werden sowohl die Ebenen der Benutzerrechte erläutert, die vom HP BladeSystem Onboard Administrator erkannt werden, als auch die ausführlichen Verfahren zur Konfigurierung der Managementfunktionen, die vom Onboard Administrator bereitgestellt werden.

Der Menüeintrag „Users/Authentication“ (Benutzer/Authentifizierung) kann nicht ausgewählt werden und zeigt keine Übersichtsinformationen zu Benutzerkonten oder -einstellungen an. Wählen Sie stattdessen die untergeordneten Menüeinträge für spezifische Einstellungen aus.

Benutzerrollen und Berechtigungsebenen

Innerhalb der Kategorie „Users/Authentication“ (Benutzer/Authentifizierung) von HP BladeSystem Onboard Administrator können Sie auf die Unterkategorie „Local Users“ (Lokale Benutzer) zugreifen. In dieser Unterkategorie können Sie Benutzerkonten zum Anmelden einzelner Personen bei HP Onboard Administrator mit einem Benutzernamen, Kennwort und typischen Kontaktinformationen erstellen. Benutzer können über eine von drei Berechtigungsebenen verfügen:

- ADMINISTRATOR ermöglicht den Zugriff auf alle Aspekte von HP BladeSystem Onboard Administrator, einschließlich Konfiguration, Firmware-Aktualisierungen, Benutzermanagement und Wiederherstellung der Standardeinstellungen.
- OPERATOR ermöglicht den Zugriff auf alle Informationen, es können jedoch nur bestimmte Konfigurationseinstellungen geändert werden. Dieses Konto ist für Personen bestimmt, die regelmäßig Änderungen an den Konfigurationseinstellungen vornehmen müssen.
- USER ermöglicht den Zugriff auf alle Informationen, jedoch können Änderungen nur im HP BladeSystem Onboard Administrator durchgeführt werden. Dieses Konto wird für Personen verwendet, die die Konfiguration des HP BladeSystem Onboard Administrator zwar einsehen müssen, jedoch nicht unbedingt zur Änderung von Einstellungen fähig sein müssen.

Der Einsatz von Berechtigungsebenen von HP BladeSystem Onboard Administrator für Benutzerebenen erleichtert die Verwaltung von Server Blade-Einschüben. Dieser Ansatz basiert auf den folgenden Grundsätzen:

- Benutzern werden Berechtigungsebenen unter „User Management“ (Benutzermanagement) zugewiesen.
- Ein Benutzer kann Zugriff auf eine beliebige Kombination aus Geräteeinschüben, Verbindungsmoduleinschüben und Onboard Administrator-Einschüben haben.

Der Zugriff auf ein Server Blade durch einen Benutzer hängt von der Berechtigungsebene ab, die dem Benutzerkonto zugeordnet wurde. Wenn Sie einen Benutzer mit Administrator ACL- oder OA-Zugriffsberechtigung auswählen, wird die Seite abgeblendet und der Zugriff auf die Blade- und Verbindungsmodul-Berechtigungen deaktiviert und es werden alle ausgewählt.

In Fällen, in denen HP SIM verwendet wird, kann Onboard Administrator in HP SIM integriert werden und mithilfe von HP SIM-Benutzern ein einmaliges Anmelden von HP SIM bei Onboard Administrator ermöglichen. Weitere Information finden Sie unter „Integration in HP SIM“.

Rollenbasierte Benutzerkonten

Rollenbasierte Benutzerkonten in Onboard Administrator dienen zwei Zwecken: Sie kontrollieren, auf welche Onboard Administrator-Funktionen ein Benutzer Zugriff hat und welche Berechtigungen auf ein temporäres Benutzerkonto in iLO übertragen werden, wenn die automatische Anmeldung verwendet wird.

Es gibt zwei wichtige Aspekte von rollenbasierten Benutzerkonten in Onboard Administrator: Einschubberechtigungen und eine Benutzerberechtigungsebene. Einschubberechtigungen bestimmen, auf welche Einschübe der Benutzer zugreifen kann. Einschubberechtigungen werden während der Erstellung des Benutzerkontos ausgewählt und gewähren Zugriff auf bestimmte Geräteeinschübe, Verbindungsmoduleinschübe oder Onboard Administrator-Einschübe. Die Berechtigungsebene bestimmt, welche Verwaltungsfunktionen der Benutzer ausführen darf. Als Benutzerberechtigungsebene kommen Administrator, Operator (Bediener) oder User (Benutzer) in Frage.

Einem Benutzer mit der Berechtigungsebene „Administrator“ und mit der Berechtigung für OA-Einschübe im Gehäuse wird automatisch uneingeschränkter Zugriff auf alle Einschübe gewährt. Er kann jede Funktion auf dem Gehäuse und auf den Einschüben ausführen, so auch das Verwalten von Benutzerkonten und das Konfigurieren des Gehäuses. Ein Benutzer mit der Berechtigungsebene „Operator“ (Bediener), der nur die Berechtigung für die OA-Einschübe hat, kann das Gehäuse konfigurieren, jedoch keine Benutzer oder Sicherheitseinstellungen verwalten und auf keine anderen Einschübe zugreifen. Ein Benutzer mit der Berechtigungsebene „User“ (Benutzer) und mit der Berechtigung für die OA-Einschübe kann nur Konfigurationseinstellungen anzeigen, diese jedoch nicht ändern. Die Benutzerkonten können mit Berechtigungen für mehrere Einschübe erstellt werden, wobei die gleiche Berechtigungsebene für den Zugriff auf alle diese Einschübe gilt.

Für Server-Administratoren können Benutzerkonten erstellt werden, die Zugriff auf Geräteeinschübe gewähren. Wenn sich der Benutzer bei Onboard Administrator anmeldet, erhält er Informationen über die gestatteten Servereinschübe. Wenn der Benutzer den iLO über die grafische Onboard Administrator-Benutzeroberfläche auswählt, wird der Benutzer automatisch bei diesem iLO mittels eines temporären Benutzerkontos angemeldet, das über dessen Berechtigungsstufe verfügt. iLO-Benutzer mit Administratorberechtigungsstufe verfügen über vollständige Kontrolle, einschließlich der Berechtigung zum Modifizieren von Benutzerkonten. Benutzer mit der Berechtigungsebene „Operator“ (Bediener) erhalten uneingeschränkte Kontrolle über die Stromversorgung und Konsolen des Servers. Benutzer mit der Berechtigungsebene „User“ (Benutzer) erhalten minimalen schreibgeschützten Zugriff auf Serverinformationen. Durch diese Funktion der einmaligen Anmeldung wird die Verwaltung mehrerer Server über die Weboberfläche von Onboard Administrator sehr vereinfacht.

Bei den Berechtigungen für Verbindungsmodule verhält sich dies etwas anders. Die automatische Anmeldung wird für Verbindungsmodule nicht unterstützt, und alle Berechtigungsebenen erhalten Zugriff auf den Link „Management Console“ für die Verbindungsmodule, für die Sie eine Berechtigung haben. Benutzer mit der Berechtigungsebene „Administrator“ oder der Berechtigungsebene „Operator“ (Bediener) können mit den virtuellen Tasten in Onboard Administrator die Stromversorgung und die UID-LED am Verbindungsmodul steuern. Benutzer mit der Berechtigungsebene „User“ (Benutzer) können nur den Status und Informationen über das Verbindungsmodul anzeigen.

Beispiele

Es folgen Beispiel einiger Management-Szenarien in einer c-Class-Umgebung und für Benutzerkonten, die erstellt werden können, um das angemessene Maß an Sicherheit zu bieten.

Szenario 1: Ein Mitglied einer Organisation benötigt uneingeschränkten Zugriff auf die Server in den Einschüben 1-8, um Protokolle einzusehen, die Stromversorgung zu steuern und die Fernkonsole zu verwenden. Der Benutzer ist jedoch nicht zur Verwaltung von Einstellungen auf Onboard Administrator berechtigt. Das Benutzerkonto zur Verwirklichung dieser Sicherheitsstufe verfügt über eine Administrator-Zugriffsebene und Berechtigung für die Servereinschübe 1-8. Der Benutzer ist folglich nicht zum Zugriff auf Onboard Administrator-Einschübe oder Verbindungsmoduleinschübe berechtigt.

Szenario 2: Ein Mitglied einer Organisation muss Ports auf zwei Verbindungsmodulen in den Einschüben 3 und 4 verwalten. Diese Person muss zwar wissen, welche Ports auf dem Switch welchen Servern zugeordnet sind, soll jedoch keine Server verwalten können. Das Benutzerkonto für diese Sicherheitsstufe verfügt über eine Benutzerzugriffsstufe, Berechtigungen für alle Servereinschübe sowie Berechtigungen für die Verbindungsmoduleinschübe 3 und 4. Dieser Benutzer kann jedoch die Stromversorgung oder UID-LED für die Verbindungsmodule oder Blades nicht steuern. Zum Steuern der Stromversorgung oder der UID-LED der Verbindungsmodule ist die Benutzerberechtigung „Operator“ (Bediener) erforderlich. Um diesen Benutzer an der Ausführung von Servervorgängen wie der Steuerung der Stromversorgung oder der Konsolen zu hindern, ist das Konto auf Einschubberechtigungen nur für die Verbindungsmodule 3 und 4 beschränkt.

Lokale Benutzer

New (Neu): Klicken Sie auf **New** (Neu), um einen neuen Benutzer zum ausgewählten Gehäuse hinzuzufügen. Der Bildschirm „Add Local User“ (Lokalen Benutzer hinzufügen) wird angezeigt.

HINWEIS: Im FIPS-Modus OFF können maximal 30 Benutzerkonten konfiguriert werden, während im FIPS-Modus ON oder DEBUG maximal 21 Benutzerkonten konfiguriert werden können. Im maximalen Benutzerkontenlimit sind reservierte Konten und die Administrator- und Virtual Connect-Konten enthalten.

Edit (Bearbeiten) – Wählen Sie einen Benutzer aus (es kann nur jeweils ein Benutzer ausgewählt werden), indem Sie das Kontrollkästchen neben dem Namen des betreffenden Benutzers markieren. Klicken Sie auf **Edit** (Bearbeiten), um die Einstellungen auf dem Bildschirm „Edit Local User“ (Lokalen Benutzer bearbeiten) zu ändern.

Delete (Löschen) – Wählen Sie den bzw. die zu löschenden Benutzer aus, indem Sie das Kontrollkästchen neben dem Namen der betreffenden Benutzer aktivieren. Um die Konten zu entfernen, klicken Sie auf **Delete** (Löschen). Bei dem Versuch, das letzte verbleibende Administratorkonto zu löschen, wird in einer Warnung darauf hingewiesen, dass das Administratorkonto nicht gelöscht werden kann, und der Löschvorgang wird abgebrochen.

Add Local User (Lokalen Benutzer hinzufügen)

Feld	Möglicher Wert	Beschreibung
Username (Benutzername)	1 bis 40 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-) und Unterstrich (_).	Im FIPS-Modus OFF können maximal 30 Benutzerkonten konfiguriert werden, während im FIPS-Modus ON oder DEBUG maximal 21 Benutzerkonten konfiguriert werden können. Im maximalen Benutzerkontenlimit sind reservierte Konten und die Administrator- und Virtual Connect-Konten enthalten. Die Benutzernamen ALL (keine Unterscheidung zwischen Groß- und Kleinschreibung), ADMINISTRATOR (keine Unterscheidung zwischen Groß- und Kleinschreibung), switch1, switch2, switch3, switch4, switch5, switch6, switch7, switch8, ldapuser, nobody tbmuser_, vcmuser und vcmuser_ sind reserviert und können nicht verwendet werden. Der Benutzername muss mit einem Buchstaben beginnen und berücksichtigt die Groß-/Kleinschreibung.
Password (Kennwort)	Im FIPS-Modus ON/ DEBUG, oder im FIPS-Modus OFF mit aktivierten starken Kennwörtern muss das Kennwort mindestens jeweils ein Zeichen von drei der vier verschiedenen Zeichentypen enthalten. Diese vier Typen sind Großbuchstaben, Kleinbuchstaben, numerisch und nicht-alphanumerisch. Das Kennwort muss zwischen 8 und 40 Zeichen lang sein. Im FIPS-Modus OFF kann das Kennwort beliebige druckbare Zeichen enthalten und es muss zwischen 3 und 40 Zeichen lang sein.	Das mit dem Benutzer verknüpfte Kennwort.
Password Confirm (Kennwortbestätigung)	Die Zeichen im Kennwort und seine Länge müssen mit den in der voranstehenden Zeile beschriebenen Kennwortregeln konform sein.	Das mit dem Benutzer verknüpfte Kennwort. Dieser Wert muss dem Wert für „Password“ (Kennwort) entsprechen.

Um die Einstellungen zu speichern, klicken Sie auf **Add User** (Benutzer hinzufügen). Der Bildschirm „Edit Local User“ (Lokalen Benutzer bearbeiten) wird angezeigt.

HINWEIS: Doppelte Benutzernamen mit unterschiedlicher Groß-/Kleinschreibung können hinzugefügt werden. Stellen Sie beim Zuweisen oder Bearbeitung der Benutzerautorisierung sicher, dass Sie den angemessenen Benutzer auswählen.

Edit Local User (Lokalen Benutzer bearbeiten)

Benutzerinformationen

Feld	Möglicher Wert	Beschreibung
Password (Kennwort)	Im FIPS-Modus ON/ DEBUG oder im FIPS-Modus OFF mit aktivierten starken Kennwörtern muss das Kennwort mindestens jeweils ein Zeichen von drei der vier verschiedenen Zeichentypen enthalten. Diese vier Typen sind Großbuchstaben, Kleinbuchstaben, numerisch und nicht-alphanumerisch. Das Kennwort muss zwischen 8 und 40 Zeichen lang sein. Im FIPS-Modus OFF mit deaktivierten starken Kennwörtern kann das Kennwort beliebige druckbare Zeichen enthalten und es muss zwischen 3 und 40 Zeichen lang sein.	Das mit dem Benutzer verknüpfte Kennwort.
Password Confirm (Kennwortbestätigung)	Die Zeichen im Kennwort und seine Länge müssen mit den in der voranstehenden Zeile beschriebenen Kennwortregeln konform sein.	Das mit dem Benutzer verknüpfte Kennwort. Dieser Wert muss dem Wert für „Password“ (Kennwort) entsprechen.
Full Name (Vollständiger Name)	0 bis 20 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Der vollständige Name des Benutzers. Alle Benutzer können ihren vollständigen Namen ändern.
Contact (Kontakt)	0 bis 20 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Kontaktinformationen für das Benutzerkonto. Bei den Kontaktinformationen kann es sich um den Namen einer Person, eine Telefonnummer oder andere nützliche Informationen handeln. Alle Benutzer können ihre eigenen Kontaktinformationen ändern.

Das Feld „Username“ (Benutzername) kann auf dem Bildschirm „Edit Local User“ (Lokalen Benutzer bearbeiten) nicht geändert werden.

Berechtigungsebene

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
Administrator	• Alle Befehle • Lokales Konto, nicht LDAP	Administrator / Administrator	Alle

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
	• Einziges Konto, das nach dem Zurücksetzen von Onboard Administrator auf die Werkseinstellungen noch verbleibt (Konto behält das konfigurierte Administratorkennwort bei) • Das Kennwort des Administratorkontos kann durch den seriellen Anschluss von Onboard Administrator mit der Wiederherstellungsoption `L` für verlorene Kennwörter zurückgesetzt werden. • Kann SSHKey herunterladen, hinzufügen und löschen. Dieser Schlüssel funktioniert nur bei dem Administrator-Konto.		
OA Administrator	• Alle Befehle • Ermöglicht den Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, darunter Konfiguration, Firmware-Aktualisierungen, Benutzerverwaltung und Standardeinstellungen.	Benutzername / Administrator	OA-Einschübe (alle automatisch ausgewählten Einschübe)
Administrator	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Administrator-Berechtigung auf Komponenten-iLO	Benutzername / Administrator	Keine OA-Einschübe und nur ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA Operator (OA Bediener)	• Ermöglicht Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, bis auf die Benutzerverwaltung	Benutzername / Operator (Bediener)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „Operator“ (Bediener) definiert*

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
Operator (Bediener)	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Operator- (Bediener-) Berechtigung auf Komponenten-iLO	Benutzername / Operator (Bediener)	Ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA User (OA-Benutzer)	• Kann Status und Informationen zum Gehäuse anzeigen • Kann den CLI-Verlauf anzeigen	Benutzername / User (Benutzer)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „User“ (Benutzer) definiert
User	• Kann Status und Informationen zu ausgewählten Einschüben anzeigen • Kann den CLI-Verlauf anzeigen • Kann ein Kennwort für das eigene Konto festlegen • Kann Benutzer-Kontaktinformationen für das eigene Konto festlegen • Kann CLI-Befehle anzeigen	Benutzername / User (Benutzer)	Keine OA-Einschübe und einige Komponenteneinschübe und Verbindungsmoduleinschübe

* EBIPA- und VLAN-Funktionen gestatten Zugriff auf alle Einschübe für einen OA-Bediener.

Die Option **User Enabled** (Benutzer aktiviert) muss ausgewählt sein, um das Benutzerkonto zu aktivieren. Wenn ein Benutzerkonto deaktiviert ist, werden alle geöffneten Sitzungen für dieses Konto beendet (abgemeldet).

Änderung der Berechtigungsebene

Wenn eine Benutzerkontoberechtigungsebene geändert wird, werden alle geöffneten Sitzungen für dieses Benutzerkonto beendet (abgemeldet). Der Benutzer muss sich nach der Änderung der Berechtigungsebene erneut anmelden.

Kontrollkästchen

Durch Aktivieren des Kontrollkästchens für den Gerätebasiseinschub wird nur dann die Benutzerberechtigung für einen Server doppelter Dichte erteilt, wenn auch A und B für diesen Einschub aktiviert werden. Markieren Sie nur A oder B für einen Geräteeinschub, um die Berechtigung auf einen einzelnen Server in einem Server Blade doppelter Dichte zu beschränken.

Benutzerberechtigungen

Kontrollkästchen	Beschreibung
Onboard Administrator Bays (Onboard Administrator-Einschübe)	Erteilt dem Benutzer Berechtigungen für die Onboard Administrator-Einschübe. Wenn als Benutzerberechtigungsebene „Administrator“ eingestellt ist, werden die Optionen „All Device Bays“ (Alle Geräteeinschübe) und „All Interconnect Bays“ (Alle Verbindungsmoduleinschübe) automatisch aktiviert, wenn „Onboard Administrator Bays“ (Onboard Administrator-Einschübe) ausgewählt wurde und alle Kontrollkästchen abgeblendet sind.
All Device Bays (Alle Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen für alle Geräteeinschübe.
Selected Device Bays (Ausgewählte Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Geräteeinschübe.
All Interconnect Bays (Alle Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen für alle Verbindungsmoduleinschübe.
Selected Interconnect Bays (Ausgewählte Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Verbindungsmoduleinschübe.

Um die Änderungen zu speichern, klicken Sie auf **Update User** (Benutzer aktualisieren).

Registerkarte „Edit Local User Certificate Information“ (Zertifikatinformationen des lokalen Benutzers bearbeiten)

Wenn die 2-Faktor-Authentifizierung aktiviert ist, wird zur Anmeldung bei dem Onboard Administrator ein Benutzerzertifikat benötigt. Benutzer mit Administratorberechtigungen können ein gültiges Zertifikat hochladen oder einem ausgewählten Benutzer zuweisen.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Nachdem das Zertifikat erfolgreich hochgeladen wurde, erscheint der SHA1-Fingerabdruck des Zertifikats.

Bei Benutzern, deren Konto bereits ein Zertifikat zugewiesen wurde, wird der SHA1-Fingerabdruck angezeigt. Jeder Benutzer mit Administratorberechtigungen kann das Zertifikat eines Benutzers löschen und ein neues Benutzerzertifikat hochladen. Wenn ein abgelaufenes Zertifikat erneuert wird, muss das erneuerte Zertifikat nicht auf den Onboard Administrator hochgeladen werden, solange das erneuerte Zertifikat die gleiche Betreffbezeichnung aufweist wie das abgelaufene Zertifikat.

Kennworteinstellungen

Auf diesem Bildschirm können Sie strenge Kennwortfunktionen geltend machen. Nur Administratoren mit Onboard Administrator-Zugriffsberechtigung sind zur Verwaltung strenger Kennwörter berechtigt.

Wählen Sie **Enable Strong Passwords** (Strenge Kennwörter aktivieren) aus, um diese Funktion zu aktivieren. Um die Einstellung zu speichern, klicken Sie auf **Apply** (Übernehmen).

HINWEIS: Diese Option kann im FIPS-Modus ON/DEBUG nicht deaktiviert werden.

Im FIPS-Modus ON/DEBUG oder bei aktivierten starken Kennwörtern muss das Benutzerkennwort drei der vier verschiedenen Zeichentypen enthalten, die in der folgenden Tabelle aufgeführt werden.

Art von Zeichen	Beschreibung
Großbuchstaben	Einen Großbuchstaben aus dem Zeichensatz A bis Z.
Kleinbuchstaben	Einen Kleinbuchstaben aus dem Zeichensatz a bis z.
Zahlen	Ein numerisches Zeichen aus dem Zeichensatz 0 bis 9.
Nicht alphanumerisches Zeichen	Ein druckbares Zeichen, bei dem es sich nicht um eine Leerstelle oder ein alphanumerisches Zeichen handelt.

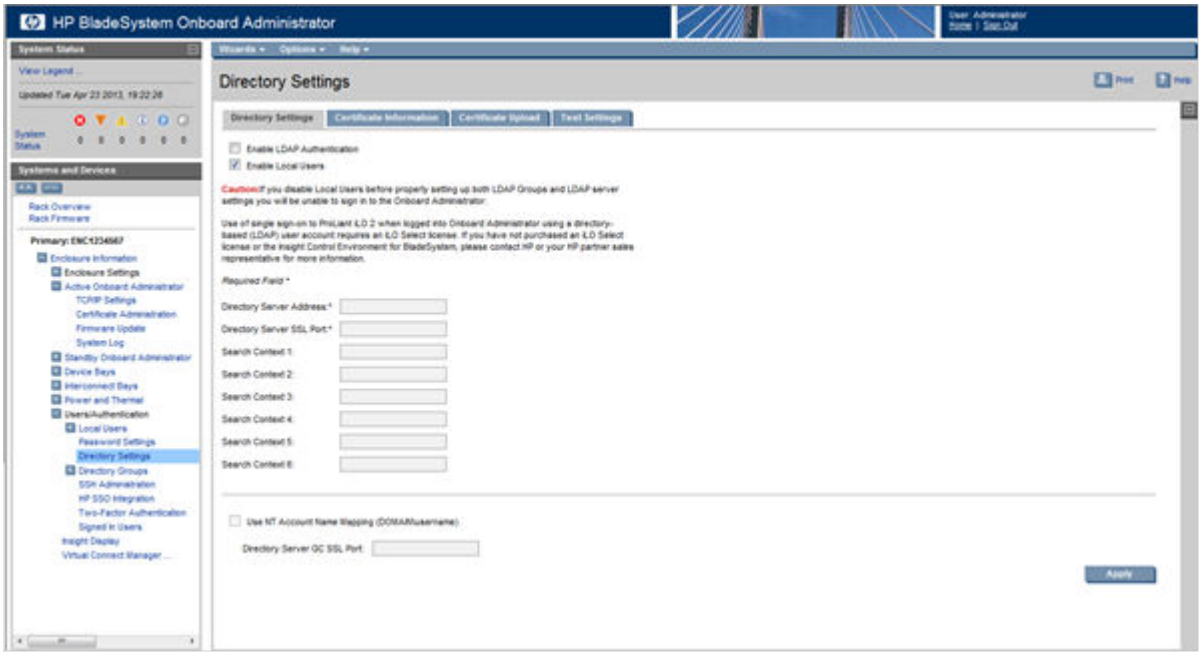
Im FIPS-Modus OFF und bei deaktivierten starken Kennwörtern kann die Mindestlänge von Kennwörtern 3 bis 40 Zeichen betragen. Wird keine Mindestlänge für Kennwörter konfiguriert, ist die Standardlänge drei Zeichen. Im FIPS-Modus ON/DEBUG oder im FIPS-Modus OFF bei aktivierten starken Kennwörtern beträgt die Mindestlänge von Kennwörtern (standardmäßig) acht Zeichen. Um die Einstellung für die Kennwortmindestlänge zu speichern, klicken Sie auf **Apply** (Übernehmen).

Bildschirm „Directory Settings“ (Verzeichniseinstellungen)

LDAP ist ein Protokoll für den Zugriff auf Informationsverzeichnisse. LDAP basiert auf dem X.500-Standard, ist jedoch wesentlich einfacher als dieser Standard. LDAP unterstützt auch TCP/IP, und ist ein offenes Protokoll.

HINWEIS: Die LDAP-Funktion von Onboard Administrator unterstützt Microsoft® Active Directory mittels des Attributs `memberOf`. Mittels des Attributs `groupMembership` wird auch Novell eDirectory unterstützt. OpenLDAP wird nicht unterstützt.

Verwenden Sie den Bildschirm „Directory Settings“ (Verzeichniseinstellungen), um den Verzeichniszugriff für die aktuell ausgewählten Gehäuse festzulegen.



- **Enable LDAP Authentication** (LDAP-Authentifizierung aktivieren) – Markieren Sie dieses Kontrollkästchen, um die Authentifizierung einer Benutzeranmeldung durch einen Verzeichnisserver zu veranlassen.
- **Enable Local Users** (Lokale Benutzer aktivieren) – Markieren Sie dieses Kontrollkästchen, um die Benutzeranmeldung mit einem lokalen Benutzerkonto anstelle eines Verzeichniskontos zu ermöglichen.
- **Search Context** (Suchkontext) – Geben Sie einen bis sechs Suchkontexte an. Ein Suchkontext ist ein Suchfilter oder eine Verknüpfung mit einem gemeinsamen Verzeichnis, durch den definiert wird, dass der Benutzer mit der Verzeichnissuche am angegebenen Pfad beginnen soll. Durch Angabe eines Suchkontexts müssen Benutzer bei der Anmeldung nicht ihre vollständigen DNs angeben. DNs können lang sein, und Benutzer kennen möglicherweise ihre DN nicht oder besitzen möglicherweise Konten in verschiedenen Verzeichniskontexten. Der Onboard Administrator versucht, den Verzeichnisdienst nach DN zu kontaktieren, und wendet dann der Reihe nach die Suchkontexte an. Dabei wird mit `Search Context 1` (Suchkontext 1) begonnen und mit allen darauf folgenden Suchkontexten fortgefahren, bis die Suche erfolgreich ist.
  - **Beispiel 1**:

    Angenommen, Sie sind `user1`. Wenn Sie als Suchkontext `ou=OU1,dc=hp,dc=com` eingeben, können Sie sich anstatt mit `cn=user1,ou=OU1,dc=hp,dc=com` mit `user1` anmelden.
  - **Beispiel 2**:

    Angenommen, die folgenden Suchkontexte sind definiert:

    - Suchkontext 1: `ou=OU1,dc=hp,dc=com`
    - Suchkontext 2: `ou=OU2,ou=OU1,dc=hp,dc=com`

    Wenn zwei Benutzer in beiden Suchkontexten den gleichen Namen `user1` besitzen und ihre Kennwörter gleich sind, dann kontaktiert Onboard Administrator bei der versuchten Anmeldung eines der beiden Benutzer immer `cn=user1,ou=OU1,dc=hp,dc=com`.

    Wenn ihre Kennwörter verschieden sind und das Kennwort für den Benutzer in `OU2` bereitgestellt wird, dann wird der von Onboard Administrator verwendete DN `cn=user1,ou=OU1,dc=hp,dc=com` zurückgewiesen, da das Kennwort nicht übereinstimmt. Bei dem nächsten Anmeldeversuch wird `cn=user1,ou=OU2,ou=OU1,dc=hp,dc=com` verwendet und er ist erfolgreich.

Der Suchkontext trifft auch auf LDAP-Verzeichnisgruppen zu, die bei der Konfiguration von verschachtelten LDAP-Gruppen hilfreich sind. Wenn der Suchkontext für eine LDAP-Verzeichnisgruppe angegeben wird, ist der genaue Kontext nicht erforderlich. Beispiel: Wenn die Position einer Gruppe ou=OU2,ou=OU1,dc=hp,dc=com ist, kann zum Auffinden diese Gruppe der Suchkontext auf höherer Ebene verwendet werden. Mit dieser Funktion lässt sich die Längenbeschränkung von Suchkontexten umgehen. Weitere Informationen zu verschachtelten Gruppen finden Sie unter „Bildschirm ‚Directory Groups'" (Verzeichnisgruppen, Verzeichnisgruppen auf Seite 335).

Feld	Möglicher Wert	Beschreibung
Directory Server Address (Verzeichnisserveradresse)	IPv4 Address (IPv4-Adresse) ###.###.###.###, wobei ### den Bereich von 0 bis 255 umfasst oder den	Die IP-Adresse, der DNS-Name oder der Name der Domäne des Verzeichnisdienstes. Ein Eintrag in diesem Feld ist erforderlich.

Feld	Möglicher Wert	Beschreibung
	DNS-Namen des Verzeichnisservers oder den Namen der Domäne angibt. IPv6-Adresse: ####:####:####:####:####:####:####:####, wobei #### im Bereich von 0 bis FFFF liegt. Eine komprimierte Version der gleichen IPv6-Adresse wird ebenfalls unterstützt.	
Directory Server SSL Port (LDAP-Port des Verzeichnisservers)	1 bis 65535	Der Port, der für die LDAP-Kommunikation verwendet wird. Port 636 ist der Standard-SSL-LDAP-Port. Ein Eintrag in diesem Feld ist erforderlich.
Search Context 1 (Suchkontext 1)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der erste durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 2 (Suchkontext 2)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der zweite durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 3 (Suchkontext 3)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der dritte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 4 (Suchkontext 4)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der vierte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 5 (Suchkontext 5)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der fünfte durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.
Search Context 6 (Suchkontext 6)	Alle Zeichen außer " (Anführungszeichen), maximal 127 Zeichen	Der sechste durchsuchbare Pfad zum Auffinden des Benutzers, wenn der Benutzer eine Authentifizierung über Verzeichnisdienste versucht. Der Pfad wird auch zur Suche nach einer verschachtelten LDAP-Gruppe verwendet.

- **Use NT Account Name Mapping (DOMAIN\username)** (NT-Kontonamenszuordnung verwenden (DOMÄNE\Benutzername)) – Markieren Sie dieses Kontrollkästchen, um die NT-Namenszuordnung zu aktivieren. Dieses Feld ermöglicht Benutzern die Anmeldung im NT-Format `domain\username`. Das Onboard Administrator-Modul kann optional für die Suche im globalen Verzeichnisserverkatalog konfiguriert werden, um die Informationen zum authentifizierten Benutzer und die entsprechenden berechtigten Gruppen zu suchen. Der standardmäßige GC SSL-Port für den Verzeichnisserver ist 3269. Dieses Feld ist optional. Wenn es nicht ausgefüllt wird, wird der globale Katalog nicht verwendet.

HINWEIS: Wenn die NT-Kontonamenszuordnung mit dem globalen Katalog verwendet und der Suchkontext nicht genügend eingeschränkt oder der Domänenname nicht angegeben wird, verknüpft das Onboard Administrator-Modul den authentifizierten Benutzer möglicherweise mit einem Benutzerkonto mit dem gleichen Namen in einer anderen Domäne. Der authentifizierte Benutzer würde dann die Autorisierung des Benutzers in der anderen Domäne erhalten. Wählen Sie Suchkontexte aus oder geben Sie den Domänennamen an, um Mehrdeutigkeiten bei der Anmeldung von LDAP-Benutzern zu vermeiden.

HINWEIS: Wenn die NT-Kontonamenszuordnung mit dem globalen Katalog verwendet wird und nicht zu einem einzelnen Benutzer aufgelöst werden kann, ist der Benutzer nicht für den Zugriff auf das Onboard Administrator-Modul berechtigt. Dies kann im Fall von Suchkontexten eintreten, die nicht genügend eingeschränkt wurden, wenn in verschiedenen Domänen mehrere Konten mit dem gleichen Namen vorhanden sind. Wählen Sie Suchkontexte aus, um Mehrdeutigkeiten zu vermeiden.

Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

HINWEIS: Die auf LDAP-Servern erzwungenen Kennwortregeln unterscheiden sich möglicherweise von den für lokale Benutzerkonten erzwungenen Kennwortregeln. Stellen Sie sicher, dass beide Regelsätze den Sicherheitsrichtlinien entsprechen.

Registerkarte „Directory Certificate Information“ (Verzeichniszertifikats-Informationen)

Dieser Bildschirm zeigt detaillierte Informationen für alle LDAP-Zertifikate an, die derzeit auf dem Onboard Administrator gelten sind.

Zeile	Beschreibung
Issued To (Ausgestellt an)	Entität, der das Zertifikat ausgestellt wurde.
Issued by (Ausgestellt von)	Die Zertifizierungsstelle, die das Zertifikat ausgestellt hat.
Valid from (Gültig ab)	Das Datum, ab dem das Zertifikat gültig ist.
Valid until (Gültig bis)	Das Datum, an dem das Zertifikat abläuft.
Serial Number (Seriennummer)	Die dem Zertifikat von der Zertifizierungsstelle zugewiesene Seriennummer.
Version	Die Versionsnummer des aktuellen Zertifikats.
MD5 Fingerprint (MD5-Fingerabdruck)	Echtheitsprüfung und ist im Zertifikat integriert
SHA1 Fingerprint (SHA1-Fingerabdruck)	Echtheitsprüfung und ist im Zertifikat integriert
Public Key (Öffentlicher Schlüssel)	Der Name des öffentlichen Schlüssels

Klicken Sie auf **Remove** (Entfernen) unterhalb des LDAP-Zertifikats, das aus dem Gehäuse entfernt werden soll.

Hochladen eines Zertifikats

Zertifikate schützen Benutzeranmeldedaten vor „Man-in-the-Middle“-Angriffen. Wenn die Zertifikate nicht auf den Onboard Administrator hochgeladen werden, kann ein „Man-in-the-Middle“ die LDAP-Anmeldeinformationen eines jeden Benutzers anzeigen, der sich bei dem Onboard Administrator anmeldet. Der Onboard Administrator akzeptiert mehrere Domänencontroller-Zertifikate, die über die

Registerkarte „Certificate Upload“ (Zertifikat-Upload) unter „Directory Settings“ (Verzeichniseinstellungen) hochgeladen werden können.

So laden Sie ein Zertifikat hoch:

1. Beziehen Sie das Zertifikat für den Domänencontroller, indem Sie einen Browser öffnen und die folgende Adresse eingeben:

   https://<Domänencontroller>:636

   wobei *Domänencontroller* die IP-Adresse für den Netzwerkdomänencontroller ist.

2. Wenn Sie zum Akzeptieren eines Zertifikats aufgefordert werden:

   - Wenn Sie Internet Explorer 6 verwenden, klicken Sie auf **Zertifikat anzeigen**.
   - Wenn Sie Internet Explorer 7 oder höher verwenden, klicken Sie auf **Laden dieser Website fortsetzen (nicht empfohlen)** und klicken Sie dann auf **Zertifikatfehler** in der oberen Adresszeile. Wählen Sie **Zertifikat anzeigen**.

3. Klicken Sie auf die Registerkarte **Details** und anschließend auf die Schaltfläche **In Datei kopieren**.

4. Wählen Sie aus der Liste der Exportoptionen „Base-64 encoded x.509 (.CER)“ (Base-64-codiert x.509 (.CER)) aus. Geben Sie einen Namen und einen Speicherort für die Datei an, und laden Sie einen Zertifikatassistenten hoch.

5. Machen Sie die exportierte Zertifikatdatei ausfindig, und benennen Sie sie in eine Datei mit der Erweiterung „.txt“ um (z. B. „dccert.txt“). Öffnen Sie die Datei in einem Texteditor, und kopieren Sie den gesamten Inhalt in die Zwischenablage. Nachstehend finden Sie ein Beispiel für eine exportierte Zertifikatdatei:

   ```
   -----BEGIN CERTIFICATE-----

   MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK

   CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is

   ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa

   Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv

   bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B

   aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y

   qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1

   lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG

   9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D

   …Ausgabe abgeschnitten…

   -----END CERTIFICATE-----
   ```

6. Kehren Sie zu Onboard Administrator zurück, fügen Sie den Inhalt des Zertifikats in das Fenster ein, und klicken Sie dann auf **Upload** (Hochladen).

Registerkarte „Directory Certificate Upload“ (Hochladen des Verzeichniszertifikats)

Auf diesem Bildschirm können Sie ein LDAP-Zertifikat zu Onboard Administrator hochladen, um eine vertrauenswürdige Beziehung mit dem LDAP-Server aufzubauen. Sie können maximal vier Zertifikate hochladen.

Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Registerkarte „Directory Test Settings“ (Verzeichnis-Testeinstellungen)

Über die Registerkarte **Test Settings** (Einstellungen testen) können Onboard Administrator-Administratoren sicherstellen, dass die bereitgestellten Konfigurationsinformationen dem Verzeichnisbenutzer den Zugriff auf Onboard Administrator und die Ressourcen im Gehäuse gewähren. Die Registerkarte **Test Settings** (Einstellungen testen) gilt nur für die aktuellen Einstellungen. Daher müssen Sie nach Vornahme von Änderung auf der Registerkarte **Directory Settings** (Verzeichniseinstellungen) zuerst auf **Apply** (Übernehmen) klicken und dann die Registerkarte **Test Settings** (Einstellungen testen) auswählen.

Auf der Registerkarte **Test Settings** (Einstellungen testen) können die Tests ausgeführt und Statusmeldungen ausgegeben werden. Wenn die Registerkarte erstmalig angezeigt wird, enthält sie eine Liste von Tests mit dem aktuellen Status `Not Run` (Nicht ausgeführt). Um die Tests auszuführen, klicken Sie auf **Test Settings** (Einstellungen testen). Die Tests werden in der angezeigten Reihenfolge ausgeführt. Die Tests werden beendet, wenn ein Fehler auftritt. Zum Durchführen der Benutzerauthentifizierung und der Benutzerauthentifizierungstests müssen Sie unter **Directory Test Controls** (Verzeichnistestkontrollen) einen Benutzernamen und ein Kennwort eingeben.

Die folgenden Tests werden in der aufgeführten Reihenfolge ausgeführt.

- **Overall Test Status (Gesamtteststatus)**

  Der Gesamtteststatus ist eine Anhäufung aller Testläufe. Mögliche Werte sind `Not Run` (Nicht ausgeführt), `Passed` (Bestanden) oder `Failed` (Fehlgeschlagen). Wird ein einzelner Test nicht bestanden, lautet der Status `Failed` (Fehlgeschlagen).

- **Ping directory Server (Anpingen des Verzeichnisservers)**

  Ein einfacher Pingtest wird ausgeführt, nachdem festgestellt wurde, dass eine gültige IP-Adresse oder ein gültiger Domänennamen für den Verzeichnisserver vorhanden ist. Der Pingtest sendet maximal vier Pingpakete an den Verzeichnisserver und meldet Erfolg oder Fehler.

  - Ein erfolgreicher Test meldet, dass Onboard Administrator einen Netzwerkpfad zum Verzeichnisserver einrichten kann.
  - Ein fehlgeschlagener Test meldet, dass Onboard Administrator keinen Netzwerkpfad zum Verzeichnisserver einrichten kann. Der Administrator sollte den Hostnamen oder die IP-Adresse überprüfen.

- **Directory Server IP Address (Verzeichnisserver-IP-Adresse)**

  Wenn die LDAP-Konfiguration eine IP-Adresse statt eines DNS angibt, überprüft dieser Test, ob die IP-Adresse eine gültige IPv4-Adresse ist. Andernfalls meldet der Test den Status `Not Run` (Nicht ausgeführt).

- Ein erfolgreicher Test meldet, dass die IP-Adresse, die für den Verzeichnisserver gespeichert wurde, eine gültige IPv4-Adresse ist.
- Ein fehlgeschlagener Test meldet, dass die IP-Adresse, die für den Verzeichnisserver gespeichert wurde, keine gültige IPv4-Adresse ist. Der Administrator muss die eingegebene IP-Adresse überprüfen und korrigieren.

- **Directory Server DNS Name (DNS-Name des Verzeichnisservers)**

  Der DNS-Suchtest stellt fest, ob Onboard Administrator den Domänennamen des LDAP-Servers auflösen kann. Wenn die LDAP-Serverkonfiguration anstatt eines DNS-Namens IP-Adressen verwendet, meldet dieser Test `Not Run` (Nicht ausgeführt).

  - Ein erfolgreicher Test meldet, dass Onboard Administrator den Directory Server-Hostnamen mit Domänennamen aufzulösen kann.
  - Ein fehlgeschlagener Test meldet, dass Onboard Administrator den Directory Server-Hostnamen nicht auflösen kann. Der Administrator muss überprüfen, ob der Verzeichnisserverhostname richtig ist und ob der Hostname für den Verzeichnisserver richtig ist.

- **Connect to Directory Server (Herstellen einer Verbindung zum Verzeichnisserver)**

  Dieser Test versucht, eine Verbindung mit der angegebenen Verzeichnisserver-IP-Adresse und dem Service-Port herzustellen.

  - Ein erfolgreicher Test meldet, dass Onboard Administrator unter dem angegebenen Hostnamen oder der angegebenen Adresse und unter der angegebenen Portnummer eine Verbindung zum Verzeichnisserver herstellen kann. Ein erfolgreicher Test bedeutet, dass der Netzwerkdienst verfügbar ist und dass der Verzeichnisdienst ausgeführt wird und auf dem angegebenen Verzeichnisserver und Port verfügbar ist.
  - Ein fehlgeschlagener Test meldet, dass Onboard Administrator keine Verbindung zum Verzeichnisserver herstellen kann. Der fehlgeschlagene Test meldet, dass der Netzwerkdienst nicht verfügbar ist. Der Administrator muss den Hostnamen oder die Adresse und die Portnummer überprüfen.

- **Connect using SSL (Herstellen einer Verbindung über SSL)**

  Dieser Test überprüft, ob der Verzeichnisserver den Verzeichnisdienst über eine SSL-Verbindung bereitstellt.

  - Ein erfolgreicher Test meldet, dass Onboard Administrator eine SSL-Verbindung zum Verzeichnisserverhostnamen oder der IP-Adresse und dem Port herstellen kann. Der Netzwerkdienst ist als sichere SSL-Verbindung verfügbar.
  - Ein fehlgeschlagener Test meldet, dass der Netzwerkdienst nicht als sichere SSL-Verbindung verfügbar ist und dass Onboard Administrator diesen Verbindungstyp nicht zulässt. Der Administrator muss einen Verzeichnisserver identifizieren, der SSL-Verbindungen unterstützt, oder den Verzeichnisserver für die Verwendung von SSL-Verbindungen neu konfigurieren.

- **Certificate of Directory Server (Zertifikat des Verzeichnisservers)**

  Wenn das Verzeichnisserver-SSL-Zertifikat auf Onboard Administrator geladen wurde, überprüfen Sie anhand dieses Tests, ob das vom Verzeichnisserver bereitgestellte Zertifikat zum aktuellen Zertifikat passt, das auf Onboard Administrator gespeichert ist. Wenn das Verzeichnisserver-SSL-Zertifikat nicht geladen wurde, dann wird dieser Test nicht ausgeführt.

- Ein erfolgreicher Test meldet, dass Onboard Administrator in der Lage war, das Verzeichnisserverzertifikat anhand der Zertifikate zu überprüfen, die auf Onboard Administrator für den angegebenen Verzeichnisserver gespeichert sind.
- Ein fehlgeschlagener Test meldet, dass das auf Onboard Administrator gespeicherte Verzeichnisserverzertifikat nicht mit dem Zertifikat übereinstimmt, das für die SSL-Verbindung bereitgestellt wurde.

- **User Authentication (Benutzerauthentifizierung)**

  Dieser Test versucht, den Benutzer mit dem unter **Directory Test Controls** (Verzeichnistestkontrollen) bereitgestellten Benutzernamen und Kennwort am Verzeichnis anzumelden. Sollte die Benutzerauthentifizierung mit dem bereitgestellten Benutzernamen und Kennwort fehlschlagen, dann wird jeder Suchkontext ausprobiert. Wenn ein Suchkontext mit dem Zeichen @ beginnt, ist der DN, der für die Anmeldung verwendet wird, der Suchname, der mit dem eingegebenen Benutzernamen verkettet ist. Andernfalls wird der Such-DN, der für die Anmeldung verwendet wird, wie folgt erstellt: `cn=<Benutzername>,<Suchkontext>`. Das Ergebnis dieses Tests identifiziert den Suchkontext, mit dem der Benutzer erfolgreich authentifiziert wurde.

- **User Authorization (Benutzerautorisierung)**

  Nachdem ein Benutzer erfolgreich authentifiziert wurde und sich an Onboard Administrator angemeldet hat, wird die konfigurierte Verzeichnisgruppe, zu der der Benutzer gehört, identifiziert. Wenn ein Benutzer zu mehreren Verzeichnisgruppen gehört, wird die Verzeichnisgruppe identifiziert, die dem Benutzer die meisten Berechtigungen erteilt.

  - Ein erfolgreicher Test meldet die Verzeichnisgruppe mit den höchsten Berechtigungsebenen für den authentifizierten Benutzer.
  - Ein fehlgeschlagener Test meldet, dass der authentifizierte Benutzer keine Autorisierung für Onboard Administrator besitzt, weil der Benutzer zu keiner der konfigurierten Verzeichnisgruppen gehört.

Test Log (Testprotokoll)

Dies ist ein laufendes Protokoll der mit den Tests verknüpften Details, die ausgeführt wurden, sowie mit den Ergebnissen dieser Tests.

Directory Test Controls (Verzeichnistest-Kontrollen)

Bevor die Benutzerauthentifizierung und die Benutzerauthentifizierungstests durchgeführt werden, werden der Benutzername und das Kennwort zur Authentifizierung zum LDAP-Server gesendet. Onboard Administrator begrenzt die Länge des Benutzernamens und des Kennworts wie angegeben. Authentifizierungsanforderungen werden vom LDAP-Server definiert. Die maximal zulässige Länge wird möglicherweise vom LDAP-Server stärker eingeschränkt als vom Onboard Administrator.

- Benutzername: Darf 0 bis 256 Zeichen lang sein.
- Kennwort: Darf 0 bis 1024 Zeichen lang sein.

Verzeichnisgruppen

Der Zugriff auf das Gehäuse kann über LDAP gewährt werden. Zur Verwendung des LDAP-Servers müssen Sie Verzeichniskonten erstellen.

Der Bildschirm „Directory Groups“ (Verzeichnisgruppen) zeigt die Verzeichnisgruppen an, die zum Gehäuse „Primary Connection“ (Hauptverbindung) hinzugefügt wurden. Sie können allen Gehäusen Benutzergruppen hinzufügen. Sie können Benutzergruppen nur im Gehäuse „Primary Connection“

(Primäre Verbindung) bearbeiten und löschen. Zur Verwendung von LDAP-Diensten müssen Sie mindestens eine Verzeichnisgruppe hinzufügen.

Spalte	Beschreibung
Kontrollkästchen	Dient zur Auswahl der Verzeichnisgruppe zum Bearbeiten oder Löschen.
Group Name (Gruppenname)	1 bis 255 Zeichen und enthält die gleichen Zeichen wie Suchkontexte. Der Gruppenname dient zur Ermittlung der Gruppenmitgliedschaft von LDAP-Benutzern. Der Gruppenname muss einer der folgenden fünf Eigenschaften einer Verzeichnisgruppe entsprechen: „Name“ (Name), „Distinguished Name“ (Eindeutiger Name), „Common Name“ (Allgemeiner Name), „Display Name“ (Anzeigename) oder „SAM Account Name“ (SAM-Konto-Name). Bei verschachtelten Gruppen basiert die Entsprechung auf `objectSid` (einem Attribut, durch das die Sicherheits-ID der Gruppe angegeben wird). Der eindeutige Name wird empfohlen, um die LDAP-Gruppe eindeutig zu bezeichnen. Wenn das Onboard Administrator-Modul für die Suche im GC-Port konfiguriert ist und kein eindeutiger Name verwendet wird, führt dies möglicherweise zu nicht korrekten Entsprechungen in verschiedenen Domänen und einer nicht beabsichtigen Autorisierung.
Privilege Level (Berechtigungsebene)	Bestimmt, welche Verwaltungsfunktionen der Benutzer ausführen darf. Als Benutzerberechtigungsebene kommen Administrator, Operator (Bediener) oder User (Benutzer) in Frage.
Description (Beschreibung)	0 bis 58 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen Die Beschreibung der LDAP-Gruppe, eine lesbarere Version des Gruppennamens oder andere nützliche Informationen.

- **New** (Neu): Klicken Sie auf **New** (Neu), um zum ausgewählten Gehäuse eine neue Verzeichnisgruppe hinzuzufügen. Sie können maximal 30 Verzeichnisgruppen hinzufügen. Der Bildschirm „Add LDAP Group“ (LDAP-Gruppe hinzufügen) wird angezeigt.
- **Edit** (Bearbeiten) – Wählen Sie eine Verzeichnisgruppe aus, die bearbeitet werden soll, indem Sie das Kontrollkästchen neben dem Namen der Gruppe aktivieren. Klicken Sie auf **Edit** (Bearbeiten), um die Einstellungen auf dem Bildschirm „Edit LDAP Group“ (LDAP-Gruppe bearbeiten) zu ändern.
- **Delete** (Löschen) – Wählen Sie eine Verzeichnisgruppe aus, die gelöscht werden soll, indem Sie das Kontrollkästchen neben dem Namen der Gruppe aktivieren. Um die Gruppe zu entfernen, klicken Sie auf **Delete** (Löschen).

Unterstützung verschachtelter LDAP-Gruppen

Bei Verwendung von Microsoft Active Directory können Sie eine oder mehrere Gruppen in einer anderen Gruppe platzieren. Gruppen, die in einer anderen Gruppe enthalten sind, werden als verschachtelte Gruppen bezeichnet. Die Gruppe, in der sich die verschachtelten Gruppen befinden, wird als Verschachtelungsgruppe bezeichnet. Verschachtelte Gruppen bieten den Vorteil, dass sich Benutzer einer verschachtelten Gruppe bei Onboard Administrator anmelden können, sofern deren Verschachtelungsgruppe entsprechend konfiguriert ist. Angenommen, `group2` ist innerhalb von `group1` verschachtelt. Benutzer in `group2` dürfen sich bei dem Onboard Administrator anmelden, sofern die übergeordnete LDAP-Gruppe (`group1`) dem Onboard Administrator hinzugefügt wird und über einen der Suchkontexte auffindbar ist. Der Suchkontext ist nicht auf die genaue Position eingeschränkt: Wenn sich der Suchkontextpfad auf einer oberen Ebene der LDAP-Verzeichnisstruktur befindet, wird die untergeordnete Verzeichnisstruktur durchsucht. Der Onboard Administrator unterstützt nur den Sicherheitsgruppentyp. Der Verteilungsgruppentyp wird nicht unterstützt.

Hinzufügen einer LDAP-Gruppe

Gruppeninformationen

HINWEIS: Es können maximal 30 Verzeichnisgruppen hinzugefügt werden.

Feld	Möglicher Wert	Beschreibung
Group Name (Gruppenname)	1 bis 255 Zeichen; alle Zeichen außer Anführungszeichen ("). Das erste Zeichen des Gruppennamens muss ein alphanumerisches Zeichen sein.	Der Gruppenname dient zur Ermittlung der Gruppenmitgliedschaft von LDAP-Benutzern. Der Gruppenname muss einer der folgenden fünf Eigenschaften einer Verzeichnisgruppe entsprechen: „Name“ (Name), „Distinguished Name“ (Eindeutiger Name), „Common Name“ (Allgemeiner Name), „Display Name“ (Anzeigename) oder „SAM Account Name“ (SAM-Konto-Name). Der eindeutige Name wird empfohlen, um die LDAP-Gruppe eindeutig zu bezeichnen. Wenn das Onboard Administrator-Modul für die Suche im GC-Port konfiguriert ist und kein eindeutiger Name verwendet wird, führt dies möglicherweise zu nicht korrekten Entsprechungen in verschiedenen Domänen und einer nicht beabsichtigen Autorisierung.
Description (Beschreibung)	0 bis 58 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Kann eine besser lesbare Version des Gruppennamens sowie andere nützliche Informationen enthalten.

Berechtigungsebene

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
Administrator	• Alle Befehle • Lokales Konto, nicht LDAP • Einziges Konto, das nach dem Zurücksetzen von Onboard Administrator auf die Werkseinstellungen noch verbleibt (Konto behält das konfigurierte Administratorkennwort bei) • Das Kennwort des Administratorkontos kann durch den seriellen Anschluss von Onboard Administrator mit der Wiederherstellungsoption `L` für verlorene Kennwörter zurückgesetzt werden. • Kann SSHKey herunterladen, hinzufügen und löschen. Dieser	Administrator / Administrator	Alle

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
	Schlüssel funktioniert nur bei dem Administrator-Konto.		
OA Administrator	• Alle Befehle • Ermöglicht den Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, darunter Konfiguration, Firmware-Aktualisierungen, Benutzerverwaltung und Standardeinstellungen.	Benutzername / Administrator	OA-Einschübe (alle automatisch ausgewählten Einschübe)
Administrator	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Administrator-Berechtigung auf Komponenten-iLO	Benutzername / Administrator	Keine OA-Einschübe und nur ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA Operator (OA Bediener)	• Ermöglicht Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, bis auf die Benutzerverwaltung	Benutzername / Operator (Bediener)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „Operator“ (Bediener) definiert*
Operator (Bediener)	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Operator- (Bediener-) Berechtigung auf Komponenten-iLO	Benutzername / Operator (Bediener)	Ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA User (OA-Benutzer)	• Kann Status und Informationen zum Gehäuse anzeigen • Kann den CLI-Verlauf anzeigen	Benutzername / User (Benutzer)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „User“ (Benutzer) definiert
User	• Kann Status und Informationen zu ausgewählten Einschüben anzeigen	Benutzername / User (Benutzer)	Keine OA-Einschübe und einige Komponenteneinschübe und Verbindungsmoduleinschübe

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
	• Kann den CLI-Verlauf anzeigen • Kann ein Kennwort für das eigene Konto festlegen • Kann Benutzer-Kontaktinformationen für das eigene Konto festlegen • Kann CLI-Befehle anzeigen		

* EBIPA- und VLAN-Funktionen gestatten Zugriff auf alle Einschübe für einen OA-Bediener.

Gruppenberechtigungen

Kontrollkästchen	Beschreibung
Onboard Administrator Bays (Onboard Administrator-Einschübe)	Erteilt dem Benutzer Berechtigungen für die Onboard Administrator-Einschübe. Wenn als Benutzerberechtigungsebene „Administrator“ eingestellt ist, werden die Optionen „All Device Bays“ (Alle Geräteeinschübe) und „All Interconnect Bays“ (Alle Verbindungsmoduleinschübe) automatisch aktiviert, wenn „Onboard Administrator Bays“ (Onboard Administrator-Einschübe) ausgewählt wurde und alle Kontrollkästchen abgeblendet sind.
All Device Bays (Alle Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen für alle Geräteeinschübe.
Selected Device Bays (Ausgewählte Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Geräteeinschübe.
All Interconnect Bays (Alle Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen für alle Verbindungsmoduleinschübe.
Selected Interconnect Bays (Ausgewählte Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Verbindungsmoduleinschübe.

Um die Einstellungen zu speichern, klicken Sie auf **Add Group** (Gruppe hinzufügen).

Bearbeiten einer LDAP-Gruppe

Gruppeninformationen

Feld	Möglicher Wert	Beschreibung
Group Name (Gruppenname)	1 bis 255 Zeichen; alle Zeichen außer Anführungszeichen ("). Das erste Zeichen des Gruppennamens muss ein alphanumerisches Zeichen sein.	Der Gruppenname dient zur Ermittlung der Gruppenmitgliedschaft von LDAP-Benutzern. Der Gruppenname muss einer der folgenden fünf Eigenschaften einer Verzeichnisgruppe entsprechen: „Name“ (Name), „Distinguished Name“ (Eindeutiger Name), „Common Name“ (Allgemeiner Name), „Display Name“ (Anzeigename) oder „SAM Account Name“ (SAM-Konto-Name). Der eindeutige Name wird empfohlen, um die LDAP-Gruppe eindeutig zu bezeichnen. Wenn das Onboard Administrator-Modul für die Suche im GC-Port konfiguriert ist und kein eindeutiger

Feld	Möglicher Wert	Beschreibung
		Name verwendet wird, führt dies möglicherweise zu nicht korrekten Entsprechungen in verschiedenen Domänen und einer nicht beabsichtigen Autorisierung.
Beschreibung	0 bis 58 Zeichen, einschließlich aller alphanumerischen Zeichen, Bindestrich (-), Unterstrich (_) und Leerzeichen.	Kann eine besser lesbare Version des Gruppennamens sowie andere nützliche Informationen enthalten.

Berechtigungsebene

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
Administrator	• Alle Befehle • Lokales Konto, nicht LDAP • Einziges Konto, das nach dem Zurücksetzen von Onboard Administrator auf die Werkseinstellungen noch verbleibt (Konto behält das konfigurierte Administratorkennwort bei) • Das Kennwort des Administratorkontos kann durch den seriellen Anschluss von Onboard Administrator mit der Wiederherstellungsoption `L` für verlorene Kennwörter zurückgesetzt werden. • Kann SSHKey herunterladen, hinzufügen und löschen. Dieser Schlüssel funktioniert nur bei dem Administrator-Konto.	Administrator / Administrator	Alle
OA Administrator	• Alle Befehle • Ermöglicht den Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, darunter Konfiguration, Firmware-Aktualisierungen, Benutzerverwaltung und Standardeinstellungen.	Benutzername / Administrator	OA-Einschübe (alle automatisch ausgewählten Einschübe)

Kontoklassifizierung	Fähigkeiten	Kontoname / Berechtigungsebene	Für dieses Konto ausgewählte Einschübe
Administrator	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Administrator-Berechtigung auf Komponenten-iLO	Benutzername / Administrator	Keine OA-Einschübe und nur ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA Operator (OA Bediener)	• Ermöglicht Zugriff auf alle Aspekte des HP BladeSystem Gehäuses und von Onboard Administrator, bis auf die Benutzerverwaltung	Benutzername / Operator (Bediener)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „Operator“ (Bediener) definiert*
Operator (Bediener)	• Kann alle Verfahren bei gestatteten Komponenteneinschüben und Verbindungsmoduleinschüben durchführen, u. a. virtueller Netzschalter und Konsolenzugriff • Operator- (Bediener-) Berechtigung auf Komponenten-iLO	Benutzername / Operator (Bediener)	Ausgewählte Komponenteneinschübe und Verbindungsmoduleinschübe
OA User (OA-Benutzer)	• Kann Status und Informationen zum Gehäuse anzeigen • Kann den CLI-Verlauf anzeigen	Benutzername / User (Benutzer)	OA Einschübe und u. U. andere ausgewählte Einschübe, die Fähigkeiten für die anderen Einschübe werden aber im „User“ (Benutzer) definiert
User	• Kann Status und Informationen zu ausgewählten Einschüben anzeigen • Kann den CLI-Verlauf anzeigen • Kann ein Kennwort für das eigene Konto festlegen • Kann Benutzer-Kontaktinformationen für das eigene Konto festlegen • Kann CLI-Befehle anzeigen	Benutzername / User (Benutzer)	Keine OA-Einschübe und einige Komponenteneinschübe und Verbindungsmoduleinschübe

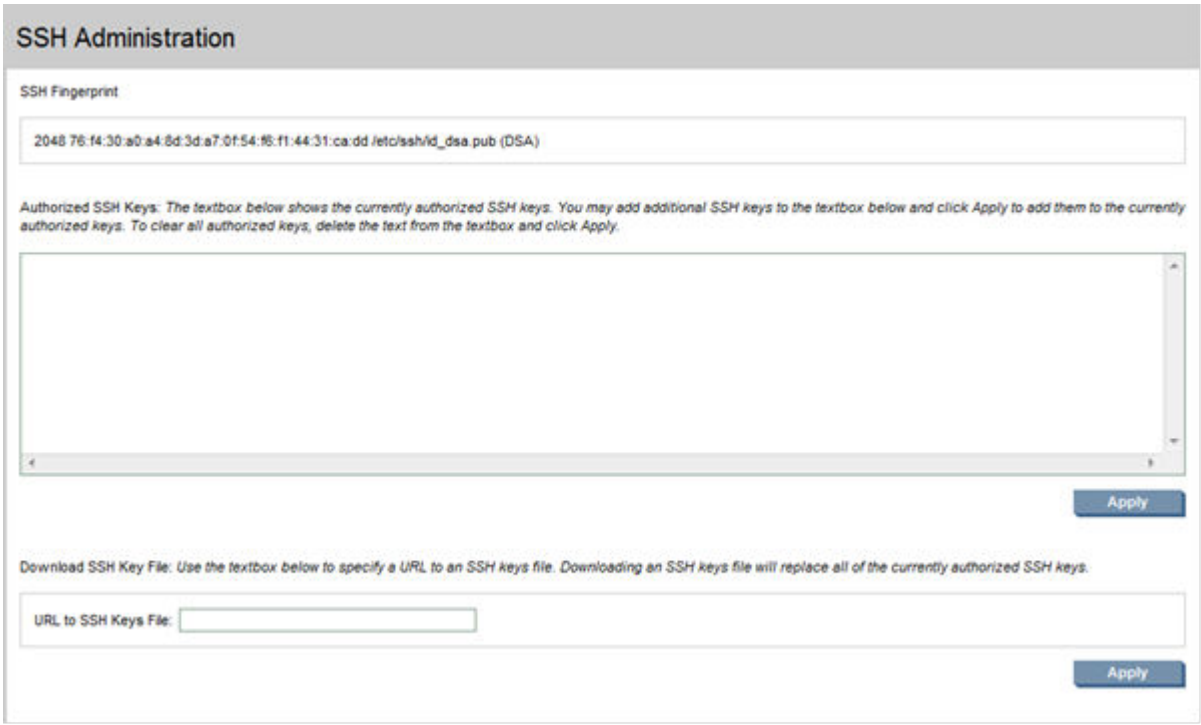
* EBIPA- und VLAN-Funktionen gestatten Zugriff auf alle Einschübe für einen OA-Bediener.

Gruppenberechtigungen

Kontrollkästchen	Beschreibung
Onboard Administrator Bays (Onboard Administrator-Einschübe)	Erteilt dem Benutzer Berechtigungen für die Onboard Administrator-Einschübe. Wenn als Benutzerberechtigungsebene „Administrator“ eingestellt ist, werden die Optionen „All Device Bays“ (Alle Geräteeinschübe) und „All Interconnect Bays“ (Alle Verbindungsmoduleinschübe) automatisch aktiviert, wenn „Onboard Administrator Bays“ (Onboard Administrator-Einschübe) ausgewählt wurde und alle Kontrollkästchen abgeblendet sind.
All Device Bays (Alle Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen für alle Geräteeinschübe.
Selected Device Bays (Ausgewählte Geräteeinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Geräteeinschübe.
All Interconnect Bays (Alle Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen für alle Verbindungsmoduleinschübe.
Selected Interconnect Bays (Ausgewählte Verbindungsmoduleinschübe)	Erteilt dem Benutzer Berechtigungen nur für die ausgewählten Verbindungsmoduleinschübe.

Um die Einstellungen zu speichern, klicken Sie auf **Update Group** (Gruppe aktualisieren).

SSH-Verwaltung


SSH Administration
SSH Fingerprint
2048 76:f4:30:a0:a4:8d:3d:a7:0f:54:f6:f1:44:31:ca:dd /etc/ssh/id_dsa.pub (DSA)
Authorized SSH Keys: The textbox below shows the currently authorized SSH keys. You may add additional SSH keys to the textbox below and click Apply to add them to the currently authorized keys. To clear all authorized keys, delete the text from the textbox and click Apply.
Apply
Download SSH Key File: Use the textbox below to specify a URL to an SSH keys file. Downloading an SSH keys file will replace all of the currently authorized SSH keys.
URL to SSH Keys File:
Apply

Diese Seite zeigt den Eigentümer jedes berechtigten SSH-Schlüssels an und ermöglicht das Hinzufügen neuer Schlüssel.

SSH Fingerprint (SSH-Fingerabdruck) – Listet den öffentlichen Teil des Paares aus öffentlichem und privatem Schlüssel auf.

Authorized SSH Keys (Berechtigte SSH-Schlüssel) – Listet die Daten der berechtigten SSH-Schlüssel auf. Der Eigentümer ist immer der Administrator. Um zusätzliche berechtigte SSH-Schlüssel hinzuzufügen, geben Sie den SSH-Schlüssel in das Textfeld ein, und klicken Sie auf **Apply** (Übernehmen). Um alle berechtigten SSH-Schlüssel zu löschen, löschen Sie den gesamten Text im Textfeld, und klicken Sie auf **Apply** (Übernehmen).

Download SSH Key File (SSH-Schlüsseldatei herunterladen) – Geben Sie Im Feld „URL to SSH Keys File“ (URL zu SSH-Schlüsseldatei) den Speicherort der öffentlichen Schlüsseldatei ein, und klicken Sie auf **Apply** (Übernehmen), um die Datei herunterzuladen. Alle aktuell berechtigten SSH-Schlüssel werden ersetzt, wenn die SSH-Schlüsseldatei heruntergeladen wird. Jeder Schlüssel ist mit dem Administratorkonto verknüpft.

HINWEIS: Wenn der Onboard Administrator im FIPS-Modus ausgeführt wird, müssen Zertifikate eine minimale RSA-Schlüssellänge von 2048 Bits aufweisen, und als Signatur-Hash-Algorithmus muss SHA-224, SHA-256, SHA-384 oder SHA-512 verwendet werden.

Unterstützte SSH- und SSL-Versionen

Onboard Administrator-Version	SSL-Version	SSH-Version
v1.20	openssl – 0.9.7k	openssh – 4.2p1
v2.00	openssl – 0.9.7l	openssh – 4.2p1
v2.30 - v2.60	openssl – 0.9.7m	openssh – 4.4p1
v3.00	openssl – fips-1.2 openssl – 0.9.8j	openssh – 5.1p1
v3.10	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v 3.20	openssl – fips-1.2 openssl – 0.9.8n	openssh – 5.1p1
v3.50 - v3.55	openssl – 0.9.8r	openssh – 5.8p2
v3.56 - v3.71	openssl – 0.9.8w	openssh – 5.8p2
v4.01 – 4.02	openssl – 0.9.8y	openssh – 5.8p2
v4.11 - v4.22	openssl – fips-2.0.5 openssl – 1.0.1e	openssh – 6.2p2
v4.30	openssl – fips-2.0.5 openssl – 1.0.1f	openssh – 6.2p2
v4.40	openssl – fips 2.0.5 openssl – 1.0.1h	openssh – 6.2p2

Integration in HP SSO

HP BladeSystem Onboard Administrator unterstützt SSO mit vertrauenswürdigen Anwendungen, z. B. HP OneView oder HP SIM. Die HP SSO-Funktion ermöglicht Ihnen, sich bei einer vertrauenswürdigen Verwaltungsanwendung anzumelden und dann automatisch auf alle verwalteten

Geräte zuzugreifen, auf denen das SSO-Zertifikat installiert ist. So konfigurieren Sie SSO für die Funktionsweise über HP SSO:

1. Stellen Sie den „SSO Trust Mode“ (SSO-Vertrauensmodus) auf „ON“ (EIN). Wählen Sie im Bildschirm „HP SSO Integration“ (Integration in HP SSO) die Option **Trust by Certificate** (Über Zertifikat vertrauen) im Dropdown-Menü **Trust Mode** (Vertrauensmodus).

HINWEIS: Wenn der Vertrauensmodus deaktiviert ist, schlägt der HP SSO-Single-Sign-On-Versuch fehl, und Sie müssen zur Anmeldung Onboard Administrator-Anmeldedaten eingeben.

HP SSO Integration
Print
Help
Settings
Certificate Information
Certificate Upload
HP SSO Trust Mode: The trust mode setting determines the manner in which the Onboard Administrator will validate a single sign-on attempt from an HP management server.
Trust mode:
Trust By Certificate
Apply

2. Wählen Sie auf dem HP SSO Integration-Bildschirm die Registerkarte **Certificate Upload** (Zertifikat-Upload) aus.
3. Laden Sie mit einer der folgenden Methoden ein Zertifikat hoch:
   - Fügen Sie den Inhalt des Zertifikats in das Textfeld ein, und klicken Sie dann auf **Upload** (Hochladen).
   - Geben Sie die IP-Adresse des HP SSO Systems ein, durch das das Gehäuse verwaltet wird, und klicken Sie auf **Apply** (Übernehmen).

HINWEIS: Onboard Administrator 4.12 und höher enthält HP SSO-Anwendungsunterstützung zur Bestimmung der Mindestanforderungen des SSO-Zertifikats.

2-Faktor-Authentifizierung

Registerkarte „Two-Factor Authentication Settings“ (Einstellungen der 2-Faktor-Authentifizierung)

HINWEIS: Bei Verwendung von Virtual Connect Manager und der 2-Faktor-Authentifizierung muss Onboard Administrator im Modus „Virtual Connect“ (Virtuelle Verbindung) konfiguriert sein.

Wenn die 2-Faktor-Authentifizierung aktiviert ist, können sich nur Benutzer mit einem gültigen Benutzerzertifikat bei Onboard Administrator anmelden. Ein gültiges Benutzerzertifikat wird von einer vertrauenswürdigen Zertifizierungsstelle signiert und dem betreffenden Benutzer auf Onboard Administrator zugeordnet.

Um die 2-Faktor-Authentifizierung für die Benutzerauthentifizierung während der Anmeldung zu aktivieren, wählen Sie **Enable Two-Factor Authentication** (2-Faktor-Authentifizierung erzwingen). Wenn die 2-Faktor-Authentifizierung aktiviert ist, ist der SSH- und Telnet-Zugriff standardmäßig deaktiviert. Durch Deaktivieren der 2-Faktor-Authentifizierung werden SSH und Telnet nicht automatisch wieder aktiviert. Sie müssen den Bildschirm „Network Access“ (Netzwerkzugriff) aufrufen und die Optionen **Enable Secure Shell** (Secure Shell aktivieren) und **Enable Telnet** (Telnet aktivieren) auswählen.

Um Onboard Administrator zu aktivieren und bei der Zertifizierungsstelle nachzuprüfen, ob das verwendete Zertifikat auf der Liste der widerrufenen Zertifikate steht, wählen Sie **Check for Certificate Revocation** (Auf Zertifikatwiderruf prüfen). Befindet sich das Zertifikat auf der Liste, wird die Anmeldung verweigert.

Feld „Certificate Owner“ (Zertifikatbesitzer)

Sie können Onboard Administrator durch Auswahl von „SAN“ so konfigurieren, dass bei der Authentifizierung von Verzeichnisbenutzern bei einem Verzeichnisserver der Hauptname des Benutzers im SAN verwendet wird, oder durch Auswahl von „Subject“ (Fach), dass der Fachname des Zertifikats verwendet wird.

Um die Einstellungen zu speichern, klicken Sie auf **Apply** (Übernehmen).

Informationen zum Konfigurieren der 2-Faktor-Authentifizierung für die Konten lokaler Benutzer und LDAP-Gruppen finden Sie unter „Erstellen von Zertifizierungsstellen und Konfigurieren der 2-Faktor-Authentifizierung für Konten lokaler Benutzer LDAP-Gruppen“ („Erstellen von Zertifizierungsstellen und Konfigurieren der 2-Faktor-Authentifizierung für lokale Benutzer- und LDAP-Gruppenkonten“ auf Seite 398).

Registerkarte „Two-Factor Authentication Certificate Information“ (Zertifikatinformationen der 2-Faktor-Authentifizierung)

Dieser Bildschirm zeigt alle Insight Remote Control-Serverzertifikate an, die der Onboard Administrator als vertrauenswürdig ansieht. Auf Onboard Administrator können von maximal 12 Zertifikate hochgeladen werden.

Zeile	Beschreibung
Certificate Version (Version des Zertifikats)	Die Versionsnummer des aktuellen Zertifikats.
Issuer Organization (Ausstellende Organisation)	Der Name der Organisation, die das Zertifikat ausgestellt hat.
Issuer Organization Unit (Ausstellende Organisationseinheit)	Der Name der Organisationseinheit, die das Zertifikat ausgestellt hat.
Issued by (Ausgestellt von)	Die Zertifizierungsstelle, die das Zertifikat ausgestellt hat.
Subject Organization (Fachorganisation)	Fachname
Issued To (Ausgestellt an)	Organisation, der das Zertifikat ausgestellt wurde.
Valid From (Gültig ab)	Das Datum, ab dem das Zertifikat gültig ist.
Valid Upto (Gültig bis)	Das Datum, an dem das Zertifikat abläuft.
Serial Number (Seriennummer)	Die dem Zertifikat von der Zertifizierungsstelle zugewiesene Seriennummer.
Extension Count (Verlängerungsanzahl)	Die Anzahl der Verlängerungen im Zertifikat.

Zeile	Beschreibung
MD5 Fingerprint (MD5-Fingerabdruck)	Anhand dieses Feldes kann die Authentizität des Zertifikats validiert werden
SHA1 Fingerprint (SHA1-Fingerabdruck)	Anhand dieses Feldes kann die Authentizität des Zertifikats validiert werden

Um ein bestehendes Zertifikat zu entfernen, klicken Sie auf **Remove** (Entfernen).

Registerkarte „Two-Factor Authentication Certificate Upload“ (Hochladen des Zertifikats der 2-Faktor-Authentifizierung)

Um die 2-Faktor-Authentifizierung zu aktivieren, müssen Sie mindestens ein gültiges Zertifikat einer Zertifizierungsstelle auf Onboard Administrator hochladen.

Es gibt zwei Methoden, um Zertifikate für die Verwendung im HP BladeSystem Onboard Administrator hochzuladen:

- Fügen Sie den Zertifikatinhalt in das Textfeld ein, und klicken Sie auf **Upload** (Hochladen).
- Fügen Sie den URL des Zertifikats in das URL-Feld ein, und klicken Sie auf **Apply** (Übernehmen).

Angemeldete Benutzer

Dieser Bildschirm zeigt alle derzeitigen Sitzungen an, die bei Onboard Administrator angemeldet sind. Dieser Bildschirm ist nur für Administratoren mit Onboard Administrator-Zugriff verfügbar. Der Administrator kann Sitzungen beenden, Benutzer deaktivieren und Benutzer auf diesem Bildschirm löschen.

Current Session (Aktuelle Sitzung) – Diese Tabelle führt die Sitzung auf, die erstellt wurde, als Sie sich bei Onboard Administrator angemeldet haben.

Other Sessions (Andere Sitzungen) – Diese Tabelle führt die anderen Benutzer auf, die bei Onboard Administrator angemeldet sind.

Spalte	Beschreibung
Kontrollkästchen	Dient zur Auswahl eines oder aller Benutzer.
Username (Benutzername)	Der Name des Benutzers, der am Gehäuse angemeldet ist.
IP Address (DNS-Adresse)	Die IP-Adresse des Benutzerkontos. Wenn die IP-Adresse der Sitzung „169.254.1.x“ ähnelt, kann es sich um die Adresse eines verbundenen Gehäuses handeln. Diese Sitzungen werden von anderen verbundenen Gehäusen erstellt. Wenn die Sitzung eines Benutzers mit der IP-Adresse eines verbundenen Gehäuses gelöscht, deaktiviert oder beendet wird, kann dies zur Folge haben, dass die Sitzungen anderer Benutzer verbundener Gehäuse ebenfalls beendet werden. Bei KVM- und seriellen Anmeldungen wird im Feld „IP Address“ (IP-Adresse) der Eintrag „Local“ (Lokal) angezeigt.
Age (Dauer)	Die in Tagen, Stunden, Minuten und Sekunden gemessene Dauer, über die hinweg das Benutzerkonto bereits angemeldet ist.
Idle Time (Inaktivitätsdauer)	Die in Tagen, Stunden, Minuten und Sekunden gemessene Dauer, über die hinweg das Benutzerkonto bereits inaktiv ist.

Spalte	Beschreibung
User Type (Art von Benutzer)	Die Art von Benutzer, der am Gehäuse angemeldet ist. Mögliche Werte sind „Local“ (Lokal), „LDAP“ oder „HP SSO“.
Session Type (Sitzungsart)	Die Art von Sitzung des angemeldeten Benutzers. Mögliche Werte sind „Web“, „SSH“, „Telnet“, „KVM“, „Serial“ (Seriell) und „Factory Diagnostics“ (Werkseitige Diagnose).
OA Module (OA-Modul)	Das Onboard Administrator-Modul, an dem der Benutzer angemeldet ist. Mögliche Werte sind „Active“ (Aktiv) oder „Standby“.

Delete Users (Benutzer löschen) – Wählen Sie den bzw. die zu löschenden Benutzer aus, indem Sie das Kontrollkästchen neben dem Namen des jeweiligen Benutzers markieren und auf **Delete Users** (Benutzer löschen) klicken. Sie können Ihr eigenes Konto oder das integrierte Administratorkonto nicht löschen.

Disable Users (Benutzer deaktivieren) – Wählen Sie den bzw. die zu deaktivierenden Benutzer aus, indem Sie das Kontrollkästchen neben dem Namen des jeweiligen Benutzers markieren und auf **Disable Users** (Benutzer deaktivieren) klicken. Sie können Ihr eigenes Konto oder das integrierte Administratorkonto nicht deaktivieren.

Terminate Sessions (Sitzungen beenden) – Wählen Sie den bzw. die Benutzer aus, deren Sitzungen beendet werden sollen, indem Sie das Kontrollkästchen neben dem Namen des jeweiligen Benutzers markieren und auf **Terminate Sessions** (Sitzungen beenden) klicken. Sie können Ihre eigene Sitzung nicht beenden.

Registerkarte „Session Options“ (Sitzungsoptionen)

Dieser Bildschirm ermöglicht es, die Zeitdauer anzugeben, für die eine Benutzersitzung gültig ist, wenn keine Aktivität ausgeführt wird. Die Sitzungen werden alle fünf Minuten überprüft, um festzustellen, ob sie für die vom Systemadministrator festgelegte Zeitdauer inaktiv waren. Waren Sitzungen für die angegebene Zeitdauer inaktiv, werden sie aus dem System entfernt.

Session Timeout (Sitzungszeitlimit): Die Anzahl der Minuten, bevor eine inaktive Sitzung ungültig wird. Für die Option „Session Timeout“ (Sitzungszeitlimit) ist jeder Wert zwischen 10 und 1440 (24 Stunden) möglich. Um das Sitzungszeitlimit zu deaktivieren, legen Sie den Wert als „0“ fest. Der Standardwert für das Sitzungszeitlimit ist 1440. Klicken Sie nach der Eingabe eines Werts für das Sitzungszeitlimit auf **Apply** (Übernehmen).

Insight Display

Alle Benutzer der grafischen Benutzeroberfläche von Onboard Administrator können auf die Insight Display-Bildschirme zugreifen, indem sie Insight Display in der Strukturansicht oder der Rack-Übersicht auswählen.

Die Registerkarte „Security“ (Sicherheit) kann die Insight Display-Tasten sperren, einen PIN-Code festlegen und den PIN-Schutz aktivieren.

HINWEIS: Wenn der Onboard Administrator mit der Einstellung ON/DEBUG für den FIPS-Modus betrieben wird, kann der PIN-Schutz nicht deaktiviert werden.

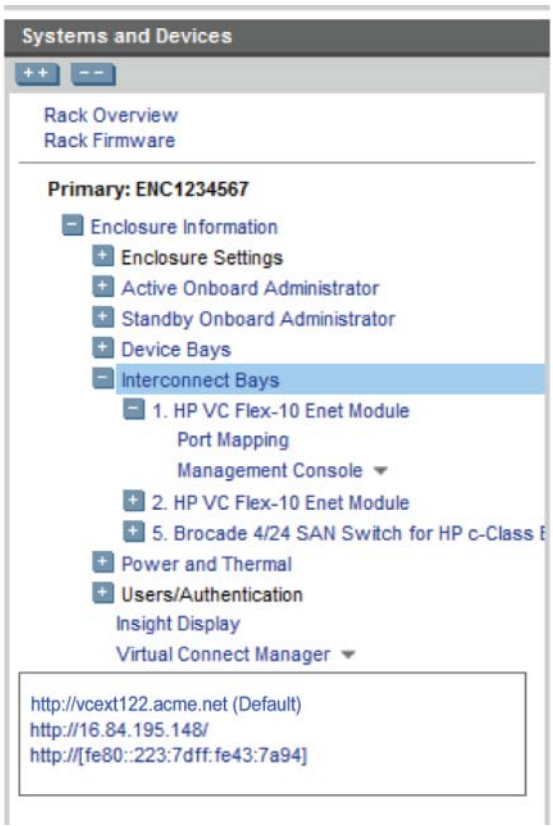
Die Registerkarte „User Note“ (Benutzernotiz) ermöglicht das Bearbeiten von Hinweistext.

Die Registerkarte „Background“ (Hintergrund) ermöglicht das Hochladen einer Windows-Bitmap-Datei mit einer Auflösung von 320x240, die als Hintergrundbild für die Benutzernotiz verwendet werden kann.

Auf der Registerkarte „Chat Mode“ (Chat-Modus) kann ein Administrator eine Unterhaltung mit einem Benutzer im Gehäuse über das Insight Display einleiten.

Virtual Connect Manager

Über den Link „Virtual Connect Manager“ (Virtueller Verbindungsmanager) im Strukturmenü wird Virtual Connect Manager in einem neuen Fenster aufgerufen. Klicken Sie zur Ansicht verfügbarer VCM-Adressen-Links (IPv4 und IPv6) auf den Abwärtspfeil neben dem Link. Wenn die FQDN-Link-Unterstützung aktiviert ist und bestimmten DNS-Konfigurations-Anforderungen entsprochen wird, wird als Standard eine FQDN-basierte Adresse angezeigt, wie in der folgenden Abbildung dargestellt. Weitere Informationen zum Aktivieren der FQDN-Link-Unterstützung finden Sie auf der Seite „Network Access“ (Netzwerkzugriff).



Weitere Informationen zur Verwendung von Virtual Connect Manager finden Sie im *HP Virtual Connect Manager User Guide* (HP Virtual Connect Manager Benutzerhandbuch).

iLO Integration

HP BladeSystem Onboard Administrator kann in das iLO eines jeden Server Blade integriert werden und ermöglicht durchgehende Authentifizierung über Onboard Administrator. Wie die CLI (Befehlszeilenschnittstelle) unterstützt HP BladeSystem Onboard Administrator nur maximal 4 gleichzeitig mit iLO verbundene Benutzer mit durchgehender Authentifizierung. Klicken Sie zum Anschließen an den iLO-Port des Server Blade auf den Link **iLO**. Wenn das Benutzerkonto auf dem iLO eingerichtet ist und mit dem Benutzerkonto des Onboard Administrator übereinstimmt, kann der Benutzer auf die iLO-GUI zugreifen, die im selben Bildschirm angezeigt wird.

Managementnetzwerk-IP-Abhängigkeiten

Der Onboard Administrator-Management-Port ermöglicht es externen Clients, über Onboard Administrator eine Verbindung mit iLOs herzustellen und Managementprozessoren zu verbinden, die für die Verwendung von Onboard Administrator-Modulen im internen Managementnetzwerk konfiguriert sind.

Die Onboard Administrator-Firmware überbrückt den Client-Verkehr zum Gehäuse vom Management-Port zum internen Gehäusemanagementnetzwerk, wenn die Ziel-IP-Adresse kein Onboard Administrator ist. Der Onboard Administrator erstellt einen Routentabelleneintrag für jede Server-iLO-IP-Adresse in einem Gehäuse. Dies befähigt Onboard Administrator zu IP-Kommunikationen mit dem betreffenden iLO. Über diese iLO 2-Routetabelleneinträge ist es möglich, jedes iLO-Netzwerk zu konfigurieren, dass sich in einem anderen Subnetz als Onboard Administrator befindet. Jedes iLO wird mit einem gültigen Gateway auf seinem Subnetz konfiguriert, auf das über eine externe Management-Port-Verbindung des Onboard Administrator-Moduls zugegriffen werden kann. In dem Netzwerk, das mit dem Onboard Administrator-Management-Port verbunden ist, werden Router benötigt, um die verschiedenen Subnetze und Gateways im Managementnetzwerk bereitzustellen. Die Verwendung anderer Subnetze zum Trennen von iLO und Onboard Administrator-Management stellt keine vollständige Isolierung dieser Netzwerke dar.

9 Verwenden der Befehlszeilenschnittstelle

Die Befehlszeilenschnittstelle

Die Onboard Administrator-Befehlszeilenschnittstelle ist über den seriellen Port von Onboard Administrator, den Management-Port, den Service-Port oder die c3000 KVM-Moduloption verfügbar und bietet Zugriff auf alle Onboard Administrator-Befehle und -Informationen.

Der Befehlszeilenschnittstellen-Benutzer muss eine gültige Kombination aus Benutzernamen und Kennwort eingeben, um sich an Onboard Administrator anzumelden. Die Befehlszeilenschnittstelle ist sowohl für lokale Benutzerkonten als auch für LDAP-Benutzer verfügbar. Die 2-Faktor-Authentifizierung ist für die Befehlszeilenschnittstelle nicht verfügbar.

Für den Zugriff auf die Onboard Administrator-Befehlszeilenschnittstelle über den Onboard Administrator-Ethernet-Management-Port oder den Service-Port müssen Telnet- oder SSH-Protokolle auf dem Onboard-Administrator aktiviert sein.

Der Zugriff auf die Onboard Administrator-Befehlszeilenschnittstelle über das c3000 KVM-Modul oder den seriellen Port von Onboard Administrator ist unabhängig von der Telnet- oder SSH-Protokolleinstellung immer verfügbar.

Für die Flash-Wiederherstellung der Onboard Administrator-Firmware oder zur Wiederherstellung eines verloren gegangenen Administratorkennworts muss der serielle Port von Onboard Administrator verwendet werden.

Die Geschwindigkeit des seriellen Anschlusses von Onboard Administrator beträgt 9600, N, 8, 1.

Weitere Informationen zur Befehlszeilenschnittstelle finden Sie im *HP BladeSystem Onboard Administrator-Befehlszeilenschnittstelle Benutzerhandbuch*.

Einrichten von Onboard Administrator mithilfe der Befehlszeilenschnittstelle

1. Stellen Sie über den seriellen Port, den Management-Port, den Service-Port oder die c3000 KVM-Moduloption eine Verbindung mit der Onboard Administrator-Befehlszeilenschnittstelle her.
2. Melden Sie sich an Onboard Administrator mit dem Benutzerkonto „Administrator“ und dem OA-Erkennungsmarken-Kennwort an.
3. Legen Sie als Onboard Administrator-Name fest: "SET OA NAME 1 <Name>".
4. Ist ein redundantes Onboard Administrator-Modul vorhanden, legen Sie als Name fest: "SET OA NAME 2 <Name>".
5. Konfigurieren Sie die Onboard Administrator-IP-Adresse.
   a. Legen Sie fest, ob die OA1/OA2-IP-Adresse oder die Gehäuse-IP-Adresse verwendet werden soll.
   b. Konfigurieren Sie die OA1-IP-Adresse als statisch oder DHCP. Beispiel für eine statische IP-Adresse: "SET IPCONFIG STATIC 1 <IP-Adresse><Netzmaske>".
6. Ist ein redundantes Onboard Administrator-Modul vorhanden: "SET IPCONFIG STATIC 2 <IP-Adresse> <Netzmaske>".

7. Legen Sie als Onboard Administrator-Gateway fest: "SET OA GATEWAY 1 <IP-Adresse>.
8. Ist ein redundantes Onboard Administrator-Modul vorhanden, legen Sie als Name fest: "SET OA GATEWAY 2 <IP-Adresse>.
9. Legen Sie die iLO-IP-Adresse fest: "SET EBIPA SERVER <IP-Adresse> <Netzmaske>. Weisen Sie jede benötigte IP-Adresse zu (bis zu 32 aufeinander folgende statische IP-Adressen).
10. Wenn das Management-Netzwerk über ein Gateway verfügt, legen Sie als IP-Adresse für das iLO Gateway fest: SET EBIPA SERVER GATEWAY <IP-Adresse>.
11. Starten Sie EBIPA FOR iLO (EBIPA FÜR iLO) folgendermaßen: "ENABLE EBIPA SERVER".
12. Beenden Sie die übrigen Einstellungen nach Bedarf. Das Befehlszeilenschnittstellen-Benutzerhandbuch gibt die Gehäusestandards für jede Einstellung an.

Konfigurieren von c-Class-iLO-IP-Adressen

Jede werksseitige c-Class-iLO-Standardkonfiguration aktiviert DHCP-Netzwerkeinstellungen. Zur Verwendung von iLO mit einem DHCP-Netzwerk schließen Sie den Onboard Administrator-Management-Port an ein Netzwerk mit einem DHCP-Server an. Onboard Administrator und alle iLO-Managementprozessoren und unterstützenden Verbindungsmodule, z. B. Virtual Connect, beziehen dann IP-Adressen vom DHCP-Server.

Um jedes iLO für statische IP-Adressen zu konfigurieren, gibt es fünf alternative Möglichkeiten. Verwenden Sie Onboard Administrator, um für jeden iLO eine IP-Adresse mit EBIPA einzurichten. Damit ist es möglich, iLO mit TCP/IP zu adressieren, so dass die Netzwerkeinstellungen neu konfiguriert werden können. Für die Alternativen 2-4 muss der Client-PC für den vorübergehenden Zugriff auf diese iLO-IP-Adressen konfiguriert werden.

Alternative 1 mit EBIPA:

Wenn für jedes iLO eine IP-Adresse mit EBIPA konfiguriert wird, wird eine feste Netzwerkkonfiguration bereitgestellt, einschließlich IP-Adresse, Netzmaske und Gateway, die auf dem Komponenteneinschub basiert, auf dem der Server installiert ist. Das neue iLO erhält die IP-Adresse für diesen Einschub, ohne dass eine weitere Konfiguration erforderlich ist.

Alternative 2 mit der OA-Befehlszeilenschnittstelle (GUI):

Melden Sie sich mit einem Konto mit Administratorrechten und Einschubsberechtigungen für das entsprechende iLO an der OA GUI an. Wählen Sie den Link **iLO** auf dem gewünschten Server, um sich mit einer einmaligen Anmeldung bei der iLO Web-GUI anzumelden. Wählen Sie **Administration | Network Settings** (Verwaltung | Netzwerkeinstellungen). Ändern Sie iLO in „DHCP disabled“ (DHCP deaktiviert), und geben Sie die gewünschten Werte für IP-Adresse, Subnetzmaske und Gateway ein. Wählen Sie **Apply** (Übernehmen). Das iLO ist nun für eine statische IP-Adresse konfiguriert. Wiederholen Sie diese Schritte für jedes iLO. Nachdem alle iLOs im Gehäuse mit statischen IP-Adressen konfiguriert wurden, schalten Sie die EBIPA-Einstellung für die Server aus.

Alternative 3 mit der OA-Befehlszeilenschnittstelle (CLI):

Melden Sie sich mit einem Konto mit Administratorrechten und Einschubsberechtigungen für das entsprechende iLO an der OA CLI an. Führen Sie den Befehl `connect server X` aus, wobei *X* die Nummer des Einschubs mit dem zu konfigurierenden iLO ist. Verwenden Sie die iLO SMASH-/CLP-Schnittstelle, um für das iLO die gewünschte IP-Adressen-Subnetzmaske und das Gateway festzulegen. Damit werden die iLO-Netzwerkeinstellungen auf die konfigurierten Werte zurückgesetzt. Wiederholen Sie diese Schritte für jedes iLO. Nachdem alle iLOs im Gehäuse mit statischen IP-Adressen konfiguriert wurden, schalten Sie die EBIPA-Einstellung für die Server aus.

Alternative 4 mit iLO 2-RIBCL-Skripten:

Erstellen Sie eine eindeutige RIBCL xml-Skript zum Konfigurieren der iLO-Netzwerkeinstellungen auf die für jedes iLO gewünschten Werte. Kopieren Sie diese Skripts an einen HTTP-, FTP- oder TFTP-Server, auf den über den Onboard Administrator zugegriffen werden kann.

Melden Sie sich mit einem Konto mit Administratorrechten und Einschubsberechtigungen für das entsprechende iLO an der OA CLI an. Führen Sie den Befehl `hponcfg X Y` durch, wobei *X* die Nummer des Einschubs mit dem zu konfigurierenden iLO und *Y* der HTTP-, FTP-, oder TFTP-Server-Netzwerkpfad zur Skriptdatei ist (z. B. hponcfg 2 http://10.128.126.204/Mod_Network_Settings.xml). Bei Verwendung von Onboard Administrator zur Ausführung des Befehls `hponcfg` wird die einmalige Anmeldungsfunktion für das ausgewählte iLO verwendet; es wird kein RIBCL-Skript mit der eindeutigen Standardkombination aus iLO-Benutzernamen und –Kennwort konfiguriert. Durch die Anwendung des RIBCL-Skripts werden die iLO-Netzwerkeinstellungen auf die konfigurierten Werte zurückgesetzt. Wiederholen Sie diese Schritte für jedes iLO. Nachdem alle iLOs im Gehäuse mit statischen IP-Adressen konfiguriert wurden, schalten Sie die EBIPA-Einstellung für die Server aus.

Alternative 5 mit dem iLO-BIOS-ROM während des Server-POST:

Verbinden Sie jeden Server mit einer KVM-Komponente. Starten Sie jeden Server neu, und beenden Sie den POST während der iLO-ROM-Initialisierung. Ändern Sie die iLO-Netzwerkkonfiguration, und geben Sie IP-Adresse, Netzmaske und Gateway manuell ein. Starten Sie den Server neu. Wiederholen Sie diese Schritte für jedes iLO.

Pinbelegungssignale für den seriellen RS232-Anschluss von Onboard Administrator

Die Pinbelegung für den seriellen DB9-Anschluss (serieller RS232-Port von Onboard Administrator), die auf dem seriellen Port von c7000 verwendet wird, ist wie folgt:

Pin	Name	Richtung	Beschreibung
1	CD	Eingang	Carrier detect (Träger erkannt)
2	RXD	Eingang	Receive data (Daten empfangen)
3	TXD	Ausgang	Transmit data (Daten senden)
4	DTR	Ausgang	Data terminal ready (Datenterminal bereit)
5	GND		System ground (Systemerdung)
6	DSR	Eingang	Data set ready (Datensatz bereit)
7	RTS	Ausgang	Request to send (Anforderung zum Senden)
8	CTS	Eingang	Clear to send (Empfangsbereitschaft)
9	RI	Eingang	Ring indicator (Aufrufsignal)

Verwenden der Service-Port-Verbindung

Der Service-Port des Onboard Administrator-Moduls ist der Gehäuse-Link-up-Anschluss, der auch ein Laptopsymbol neben dem Pfeil nach oben besitzt. Wenn die Gehäuse-Link-Anschlüsse zur Verbindung von Gehäusen verwendet werden, ist der oberste Gehäuse-Link-up-Anschluss der Service-Port für alle verbundenen Gehäuse. Dieser Port ist eine 100BaseT-Ethernet-Buchse und kann über ein Standard-CAT5-Patch-Kabel direkt mit einem Laptop- oder PC-RJ45-Ethernet-Anschluss verbunden werden, da die Verdrahtung am Link-up-Anschluss als Crossover ausgeführt ist und so die direkte Verbindung mit einem 100BaseT-Anschluss an einem PC zulässt.

Der Service-Port stellt eine direkte Verbindung zu jedem der aktiven Onboard Administrator-Module in allen verbundenen Gehäusen her oder nur zu dem aktiven Onboard Administrator-Modul in einem einzelnen Gehäuse, wenn keine anderen verbundenen Gehäuse vorhanden sind. Die Netzwerkverbindung zu den Gehäusen ist privat und kann nicht für den Zugriff auf Komponenten außerhalb des internen Gehäusemanagementnetzwerks verwendet werden. Sie kann für den direkten Zugriff auf den aktiven Onboard Administrator an der aktiven Service-IP-Adresse verwendet werden, die auf dem Gehäuse-Info-Bildschirm dieses Gehäuse-Insight Display gefunden wird.

Für den Laptop oder PC, der an den Gehäuse-Service-Port angeschlossen wird, muss DHCP für die Netzwerkverbindung aktiviert sein. Der Laptop oder PC bezieht nach einem DHCP-Timeout eine konfigurationsfreie IP-Adresse im Bereich 169.254.x.y, wenn auf dem Laptop oder PC Windows ausgeführt wird. Wenn auf dem Laptop oder PC Linux ausgeführt wird, müssen Sie unter Umständen den Netzwerkport manuell auf 169.254.2.1 mit der Netzmaske 255.255.0.0 festlegen.

Zum Zugriff auf die grafische Benutzeroberfläche eines aktiven Onboard Administrator-Moduls: Verwenden Sie die Service-IP-Adresse des aktiven OA vom Insight Display des betreffenden Gehäuses als Webadresse im Browser Ihres Laptops oder PCs. Melden Sie sich am OA mit einem konfigurierten Benutzerkonto und Kennwort an.

Zum Zugriff auf die CLI eines aktiven Onboard Administrator-Moduls: Verwenden Sie basierend auf den konfigurierten Netzuwerkzugriffseinstellungen ein Telnet- oder SSH-Programm und stellen Sie eine Verbindung zur Service-IP-Adresse des aktiven OA her. Melden Sie sich am OA mit einem konfigurierten Benutzerkonto und Kennwort an.

Da keiner der konfigurierten Geräteeinschubs-iLOs über eine IP-Adresse im konfigurationsfreien IP-Adressen-Bereich verfügt, müssen Sie auf dem Laptop oder PC manuell eine Netzwerkroute hinzufügen, wenn Sie über den Service-Port auf die iLO-IP-Adresse zugreifen müssen. Bei Verwendung einer Windows-Laptop- oder -PC-Befehlsshell ist die Syntax wie folgt:

route add iLO_IP_address mask 255.255.255.255 OA_service_IP_address

Nachdem dem Laptop oder dem PC die Route zu einem iLO hinzugefügt wurde, kann über die grafische Benutzeroberfläche des OA oder direkt über SSH auf den iLO zugegriffen werden.

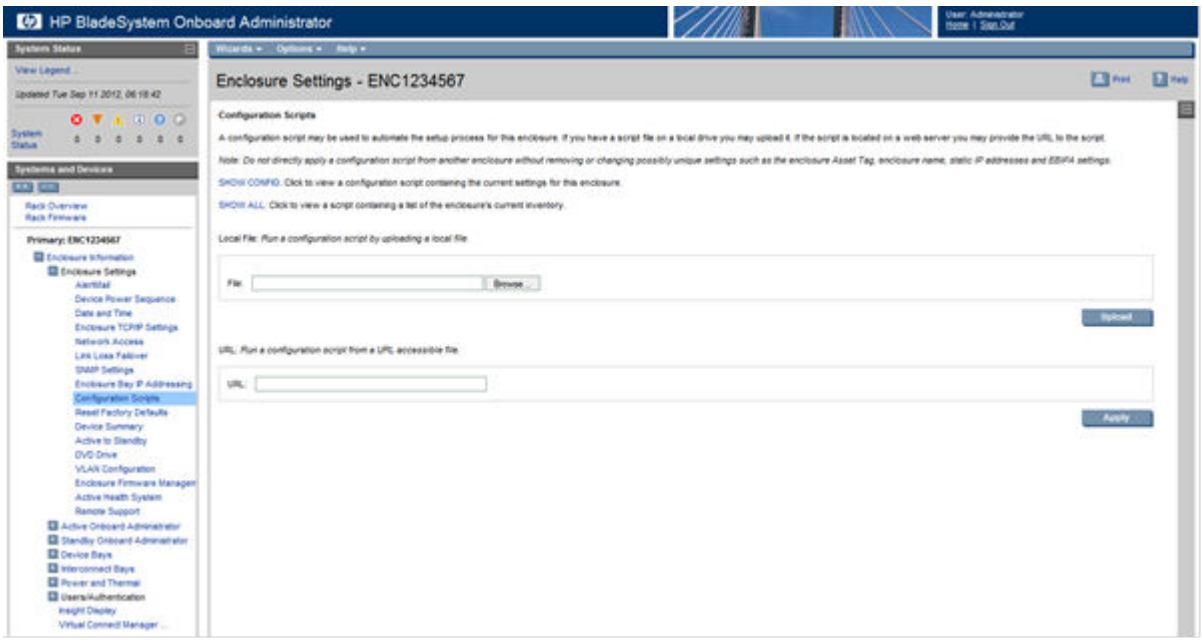
Der aktive Onboard Administrator unterstützt nicht das Weiterleiten vom Service-Port zu einem Verbindungsmodul-Managementprozessor. Wenn jedoch das Verbindungsmodul die serielle Verbindung zum OA unterstützt, kann der Befehl „connect interconnect“ der OA-Befehlszeilenschnittstelle verwendet werden, um eine Verbindung mit einem Verbindungsmodul herzustellen.

Die Service-Port-Verbindung ist nur als temporäre Ethernet-Verbindung zum privaten Netzwerk des Gehäuses gedacht, um das Trennen der Verbindung des Management-Ports mit dem externen Managementnetzwerk beim Zugriff auf Onboard Administrator während eines Wartungsereignisses zu vermeiden.

Verwenden von Konfigurationsskripts

Konfigurationsskripts

Verwenden Sie zur Verwaltung der Einstellungen und Konfigurationsinformationen Konfigurationsskripts, insbesondere beim Konfigurieren von mehreren Gehäusen und Onboard Administrator-Modulen. Auf diese Weise brauchen die einzelnen Gehäuse nicht manuell konfiguriert werden. Konfigurationsskripts können mit Onboard Administrator im Browser oder über die Befehlszeilenschnittstelle erstellt und verwendet werden. Dasselbe ist auch über die CLI möglich, wobei die Konfigurationsskripts dann wie Shell-Skripts unter Linux oder UNIX ausgeführt werden.



Aktuelle Konfiguration

So zeigen Sie eine aktuelle Konfiguration für das Gehäuse an:

1. Klicken Sie auf den Link **SHOW CONFIG** (Konfiguration anzeigen). Die Konfiguration wird in einem neuen Browserfenster geöffnet.
2. Um die Konfiguration als Textdatei zu speichern, wählen Sie eine der folgenden Optionen aus:
   - Wählen Sie bei Verwendung von Microsoft Internet Explorer die Option **Speichern unter** aus.
   - Wählen Sie bei Einsatz von Mozilla Firefox die Option **Seite speichern unter**.
   - Wählen Sie bei Verwendung von Google Chrome die Option **Save Link As** (Link speichern unter) aus.

Sie können zudem eine lokale Datei oder einen URL für das Konfigurationsskript auswählen.

- **Local file** (Lokale Datei): Durchsuchen Sie die Verzeichnisstruktur nach der Konfigurationsdatei oder geben Sie den Pfad der Konfigurationsdatei in das Textfeld ein. Die maximale Anzahl von Zeichen im Dateipfad ist 256. Geben Sie nach der Eingabe des Pfads für die Konfigurationsdatei auf **Upload** (Hochladen).
- **URL**: Geben Sie in Form einer Internetadresse (HTTP://) einen Pfad zur Konfigurationsdatei ein, wenn sich die Konfigurationsdatei auf einem Webserver befindet. Die maximale Anzahl von

Zeichen im Dateipfad ist 256. Geben Sie den URL ein, und klicken Sie dann auf **Apply** (Übernehmen).

Aus Sicherheitsgründen enthält die abgerufene aktuelle Konfiguration keine Benutzerkennwörter. Sie können das Skript manuell bearbeiten und nach dem Benutzernamen in den ADD USER-Zeilen die Benutzerkennwörter einfügen. Außerdem enthält die abgerufene aktuelle Konfiguration keine der LCD-Einstellungen für „Lock Buttons“ (Tasten sperren), „Enable PIN Protection“ (PIN-Schutz aktivieren) und „PIN Code“ (PIN-Code). Diese Einstellungen können nicht aus dem Konfigurationsskript eingefügt werden.

Aktueller Gehäusebestand

Um einen Skript des aktuellen Gehäusebestands anzuzeigen, klicken Sie auf den Link **Show All** (Alles anzeigen). Der aktuelle Gehäusebestand wird in einem neuen Browser-Fenster geöffnet. Um den Bestand als Textdatei zu speichern, wählen Sie eine der folgenden Optionen:

- Wählen Sie bei Verwendung von Microsoft Internet Explorer die Option **Speichern unter** aus.
- Wählen Sie bei Einsatz von Mozilla Firefox die Option **Seite speichern unter**.
- Wählen Sie bei Verwendung von Google Chrome die Option **Save Link As** (Link speichern unter) aus.

Der heruntergeladene Text liefert die gleichen Informationen wie der CLI-Befehl `SHOW ALL`. Aus der Textdatei geht zudem die aktuelle Konfiguration für das Gehäuse hervor.

HINWEIS: Es dauert möglicherweise einige Minuten, bis die Gehäusebestandsinformationen im neuen Browser-Fenster geladen werden. Sie müssen warten, bis der Befehl `Variable list` (Variablenliste) angezeigt wird.

USB-Unterstützung

Dieses Feld wird angezeigt, wenn ein USB-Schlüssel im aktiven Onboard Administrator-USB-Port erkannt wird und Konfigurationsdateien vorhanden sind. Um eine Konfigurationsdatei herunterzuladen, wählen Sie im Menü eine Datei aus, und klicken Sie anschließend auf **Apply** (Übernehmen). Die maximale unterstützte USB-Schlüsselgröße ist 4 GB.

Geben Sie zum Speichern der aktuellen Onboard Administrator-Konfigurationsdatei auf dem USB-Schlüssel einen einfachen Dateipfad ein, und zwar entweder einen relativen Pfad im Format `Pfad/Datei` oder mit einem führenden Punkt (.) wie z. B. `./path/file` oder einen absoluten Pfad beginnend mit einem Schrägstrich (/) im Format `/Pfad/Datei`. Geben Sie keine URL ein. Der Dateiname darf keine Leerzeichen enthalten. Klicken Sie auf **Apply** (Übernehmen).

Werkseinstellungen wiederherstellen

HINWEIS: Wenn sich das Gehäuse im VC-Modus befindet, müssen Sie den Modus löschen, bevor Sie die Werkseinstellungen wiederherstellen.

HINWEIS: Speichern Sie die Konfiguration, bevor Sie die Werkseinstellungen wiederherstellen. Klicken Sie auf **SHOW CONFIG**, um ein Skript mit der aktuellen Konfiguration herunterzuladen. Mit Hilfe dieses Skripts können Sie zu einem späteren Zeitpunkt die Einstellungen wiederherstellen, die beim Zurücksetzen auf die Werkseinstellungen verloren gegangen sind.

HINWEIS: Nach dem Zurücksetzen auf die Werkseinstellungen sind die IPv6-Netzwerkeinstellungen (IPv6, SLAAC und DHCPv6) des Gehäuses standardmäßig aktiviert.

Wenn Sie das Gehäuse auf die Werkseinstellungen zurücksetzen, werden alle Gehäuseeinstellungen bis auf das integrierte Administratorkennwort zurückgesetzt. Alle AlertMail-, Netzwerk-, Netzwerkprotokoll-, SNMP- und Power-Management-Einstellungen werden zurückgesetzt.

Um das Gehäuse zurückzusetzen, klicken Sie auf **Reset Factory Defaults** (Werkseinstellungen wiederherstellen). Ein Bestätigungsfenster wird angezeigt. Um das Zurücksetzen des Gehäuses zu bestätigen, klicken Sie auf **OK**, oder um den Vorgang zu beenden, ohne das Gehäuse auf die Werkseinstellungen zurückzusetzen, klicken Sie auf **Cancel** (Abbrechen).

HINWEIS: Diese Funktion ist im FIPS-Modus ON/DEBUG deaktiviert.

So zeigen Sie eine aktuelle Konfiguration für das Gehäuse an:

1. Klicken Sie auf den Link **SHOW CONFIG** (Konfiguration anzeigen). Die Konfiguration wird in einem neuen Browserfenster geöffnet.
2. Um die Konfiguration als Textdatei zu speichern, wählen Sie eine der folgenden Optionen aus:
   - Wählen Sie bei Verwendung von Microsoft Internet Explorer die Option **Speichern unter** aus.
   - Wählen Sie bei Einsatz von Mozilla Firefox die Option **Seite speichern unter**.
   - Wählen Sie bei Verwendung von Google Chrome die Option **Save Link As** (Link speichern unter) aus.

Aus Sicherheitsgründen enthält die abgerufene aktuelle Konfiguration keine Benutzerkennwörter. Sie können das Skript manuell bearbeiten und nach dem Benutzernamen in den ADD USER-Zeilen die Benutzerkennwörter einfügen. Außerdem enthält die abgerufene aktuelle Konfiguration keine der LCD-Einstellungen für „Lock Buttons“ (Tasten sperren), „Enable PIN Protection“ (PIN-Schutz aktivieren) und „PIN Code“ (PIN-Code). Diese Einstellungen können nicht über das Konfigurationsskript hinzugefügt werden.

Bei Löschen des VC-Modus werden alle VC-Einstellungen vom Gehäuse gelöscht. Schalten Sie vor Löschen des VC-Modus alle VC-konfigurierten Server aus. Server, die nicht ausgeschaltet werden, behalten möglicherweise ihre VC-Einstellungen bei, bis sie neu gestartet werden. Der VC-Modus muss gelöscht werden, bevor zum FIPS-Modus OFF/ON/DEBUG gewechselt wird.

So löschen Sie den VC-Modus:

1. Klicken Sie auf **Clear VC Mode** (VC-Modus löschen). Es wird ein Bestätigungsbildschirm mit folgender Meldung angezeigt: `All servers should be powered off and not configured by Virtual Connect prior to clearing VC mode. Are you sure that you wish to clear VC mode?`
2. Klicken Sie auf **OK**.

10 Unterstützung für HP Integrity i2 Server Blades

Aktualisierte Unterstützung für HP Integrity BL860c i2, BL870c i2 und BL890c i2 Server Blades

Die HP Integrity i2 Server Blades umfassen BladeLink-Hardwarebaugruppen, die mehrere BL860c i2 Server Blades miteinander verbinden, um so Dual-Blade-Vier-Sockel- und Quad-Blade-Acht-Sockel-Server zu erstellen.

Zur Unterstützung dieser Server Blades wird Onboard Administrator-Firmwareversion 3.00 oder höher benötigt.

Die Strukturansicht und die grafische Ansicht der Benutzeroberfläche von Onboard Administrator wurden zur Unterstützung von HP Integrity i2 Server Blades aktualisiert. Die Bildschirme „Port Mapping“ (Port-Zuordnung), „Firmware“ und „Partner Blade“ (Partner-Blade) wurden ebenfalls aktualisiert.

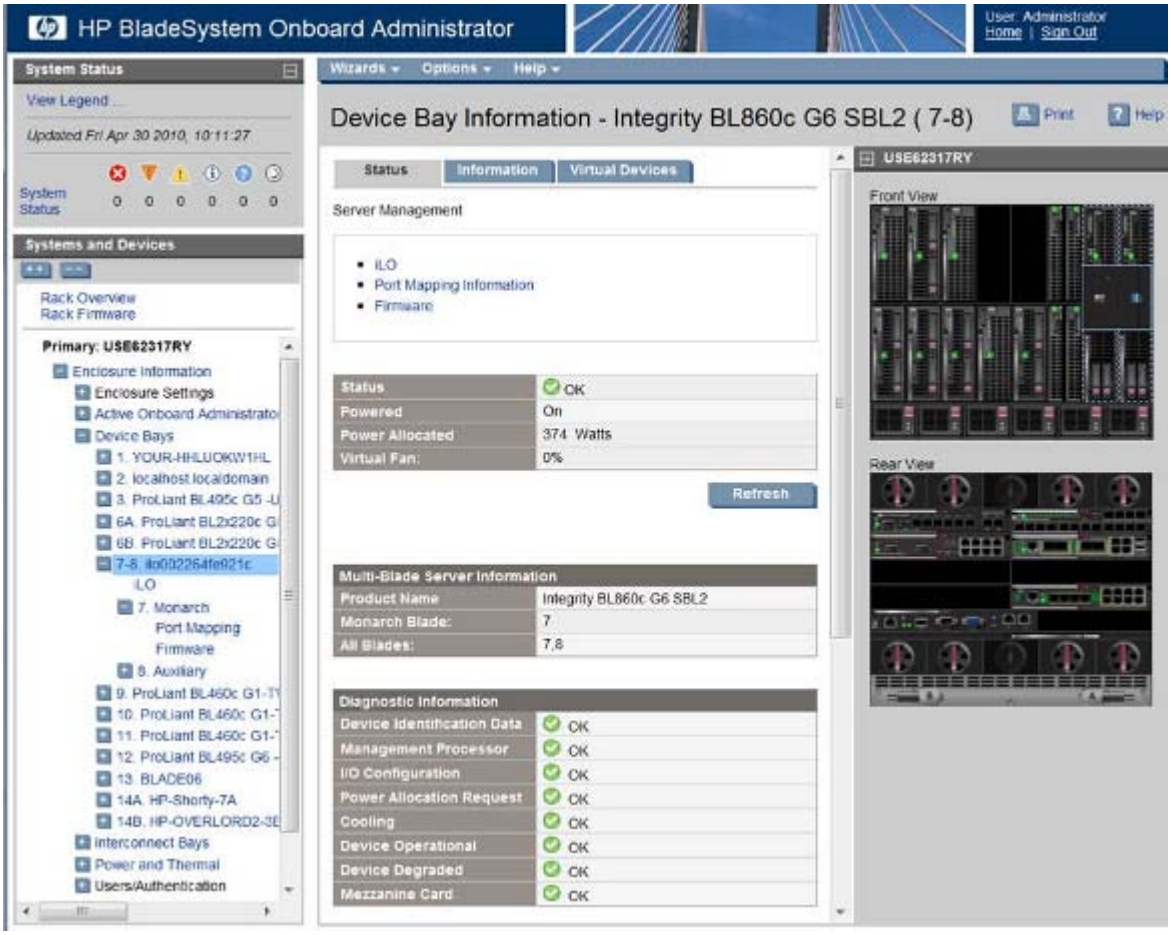
Änderungen der Strukturansicht und der grafischen Ansicht für HP Integrity i2 Server Blades

Alle HP Integrity i2 Server Blades besitzen BladeLink-Hardware. Der Haupteintrag der Strukturansicht eines verbundenen Server Blade zeigt den Bereich der Einschübe mit allen einzelnen Server Blades an, die miteinander verbunden sind.

Wird der Haupteintrag der Strukturansicht für den verbundenen Server Blade ausgewählt, dann wird die BladeLink-Hardware in der grafischen Ansicht durch ein blaues durchgezogenes Kästchen hervorgehoben. Die einzelnen miteinander verbundenen Server Blades und zugehörigen Partner-Blades werden einzeln durch gepunktete blaue Kästchen markiert. Die als Titel angezeigten Geräteeinschubs-Informationen geben die Größe der BladeLink-Hardware und den Bereich der Einschübe im verbundenen Server an.

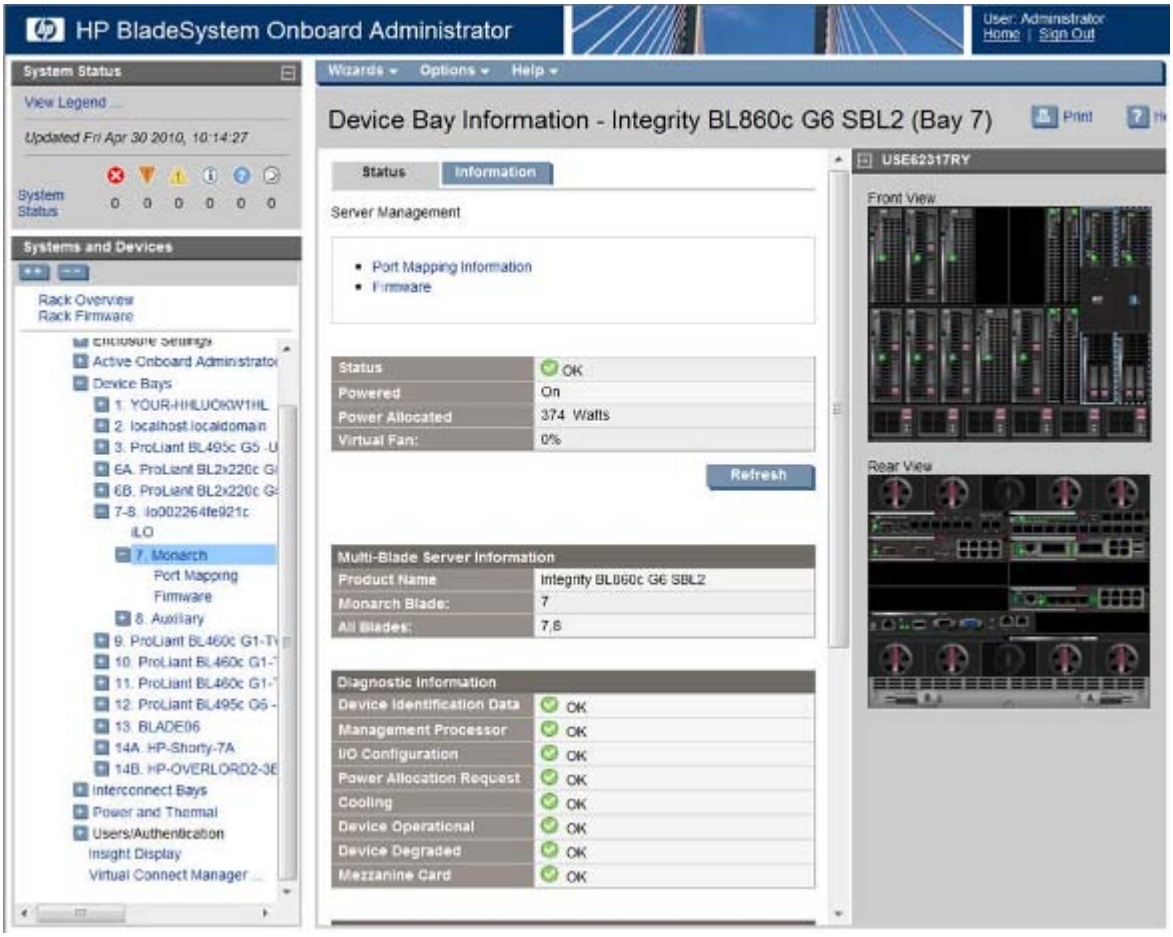
Die Registerkarte „Device Bay Information Virtual Device“ (Geräteeinschubs-Informationen – Virtuelles Gerät) ist nur auf dem Haupteintrag der Strukturansicht für den gesamten verbundenen Server Blade verfügbar.

Der iLO-Eintrag in der Strukturansicht ist nur unter dem Haupteintrag für den gesamten verbundenen Server Blade verfügbar.



Unter dem iLO-Eintrag des verbundenen Server Blade wird je nach der Rolle des betreffenden Server Blade im verbundenen Server ein neuer Eintrag namens „Monarch“ oder „Auxiliary“ (Zusatz) zur Strukturansicht hinzugefügt.

Bei Auswahl von „Monarch“ bzw. „Auxiliary“ (Zusatz) wird die Geräteeinschubs-Informationsseite für den betreffenden Server Blade geöffnet. Der ausgewählte Blade besitzt in der grafischen Ansicht eine durchgezogene blaue Hervorhebung. Die anderen verbundenen Server Blades und alle zugehörigen Partner-Blades besitzen gepunktete blaue Hervorhebungen. Die Tabelle „Multi-Blade Server Information“ (Multi-Blade-Serverinformationen) gibt den Produktnamen und den Monarch-Einschub an und führt zudem alle Server Blade-Einschübe des verbundenen Servers auf.



Änderungen der Portzuordnung für HP Integrity i2 Server Blades

Die Portzuordnung für verbundene Server Blades wird auf jedem einzelnen Server Blade angezeigt, der in der Strukturanzeige unter der Rolle „Monarch“ oder „Auxiliary“ (Zusatz) für den betreffenden Server Blade ausgewählt wurde.

Partner-Blade-Änderungen für HP Integrity i2 Server Blades

Ein verbundener HP Integrity i2 Server Blade kann maximal über drei Partner-Blades verfügen. Weitere Informationen finden Sie im *HP Integrity i2 Server Blade Installation Guide* (HP Integrity i2 Server Blade Installationshandbuch) (http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?lang=en&cc=us&prodClassId=-1&contentType=SupportManual&docIndexId=3124&prodTypeId=3709945&prodSeriesId=4186432).

11 Fehlerbeseitigung

Fehlermeldungen im Onboard Administrator

- SOAP-Antwortfehler: Hierbei handelt es sich um allgemeine Fehler, die vom gSoap-Dienst bei Prüfungsfehlern, Komponentenausfällen usw. gemeldet werden. Diese Fehler werden in zwei Kategorien eingeteilt:
  - Benutzeranfrage-Fehler
  - Onboard Administrator-Fehler
- SOAP-Schnittstellenfehler: Diese Fehler signalisieren interne Probleme mit dem gSoap-Dienst.
- CGI-Anwendungsfehler: Diese Fehler werden von einzelnen CGI-Prozessen gemeldet. Jede davon gibt ihre eigenen Fehler aus:
  - Dateiuploadfehler
  - Insight Display-Screenshotfehler

Onboard Administrator-Fehler

1 The submitted user already exists. (Der übermittelte Benutzer existiert bereits.)

2 The submitted user name is not valid. (Der übermittelte Benutzername ist ungültig.)

3 The maximum number of users already exists. (Die maximale Anzahl von Benutzern existiert bereits).

5 The requested user does not exist. (Der angeforderte Benutzer existiert nicht).

6 The submitted group already exists. (Die übermittelte Gruppe existiert bereits).

7 Invalid privilege level. (Ungültige Berechtigungsebene).

8 Insufficient privileges for the requested operation. (Unzureichende Berechtigungen für den angeforderten Vorgang).

10 The submitted user was already enabled. (Der übermittelte Benutzer wurde bereits aktiviert).

11 The submitted user was already disabled. (Der übermittelte Benutzer wurde bereits deaktiviert).

12 The submitted user already has administrator rights. (Der übermittelte Benutzer verfügt bereits über Administratorrechte).

13 The submitted user is not an administrator. (Der übermittelte Benutzer ist kein Administrator).

14 An error occurred while creating a group entry. (Beim Erstellen eines Gruppeneintrags ist ein Fehler aufgetreten).

16 Unable to perform the operation. (Der Vorgang kann nicht durchgeführt werden.) Retry the operation or restart OA. (Vorgang wiederholen oder OA neu starten.) (System Error 16) (Systemfehler 16)

17 Unable to perform the operation. (Der Vorgang kann nicht durchgeführt werden.) Retry the operation or restart OA. (Vorgang wiederholen oder OA neu starten.) (System Error 17) (Systemfehler 17)

18 Unable to perform the operation. (Der Vorgang kann nicht durchgeführt werden.) Retry the operation or restart OA. (Vorgang wiederholen oder OA neu starten.) (System Error 18) (Systemfehler 18)

19 The submitted bay is already assigned. (Der übermittelte Einschub ist bereits zugewiesen).

20 The submitted bay is not assigned. (Der übermittelte Einschub ist nicht zugewiesen).

22 The submitted value is already in use. (Der übermittelte Wert wird bereits verwendet).

23 The first character in the submitted value is not valid. (Das erste Zeichen im übermittelten Wert ist ungültig).

24 The submitted value contains an invalid character. (Der übermittelte Wert enthält ein ungültiges Zeichen).

25 The submitted value is too short. (Der übermittelte Wert ist zu kurz).

26 The submitted value is too long. (Der übermittelte Wert ist zu lang).

27 The submitted trap receiver already exists. (Der übermittelte Trap-Empfänger existiert bereits).

28 The maximum number of trap receivers already exists. (Die maximale Anzahl von Trap-Empfängern existiert bereits).

29 The maximum number of IP managers already exists. (Die maximale Anzahl von IP-Managern existiert bereits).

30 The IP Manager already exists. (Der IP-Manager existiert bereits).

31 The submitted bay number is out of range. (Die übermittelte Einschubnummer befindet sich außerhalb des gültigen Bereichs).

32 The submitted IP address is not valid. (Die übermittelte IP-Adresse ist ungültig).

33 The submitted value is null. (Der übermittelte Wert ist null).

34 An error occurred while generating an event. (Beim Generieren eines Ereignisses ist ein Fehler aufgetreten).

35 An error occurred opening the enclosure system log. (Beim Öffnen des Gehäuse-Systemprotokolls ist ein Fehler aufgetreten).

36 The submitted date and/or time value was not formatted correctly. (Der übermittelte Datums- und/oder Zeitwert hatte nicht das korrekte Format).

37 An error occurred while opening the Onboard Administrator's system log. (Beim Öffnen des Systemprotokolls von Onboard Administrator ist ein Fehler aufgetreten).

38 The NMI Dump failed for the submitted blade. (Der NMI-Dump ist für das übermittelte Blade fehlgeschlagen).

39 Setting the UID for the submitted blade failed. (Das Festlegen der UID für das übermittelte Blade ist fehlgeschlagen).

40 Setting the environment variable for the submitted blade failed. (Das Festlegen der Umgebungsvariable für das übermittelte Blade ist fehlgeschlagen).

41 Setting the boot order for the submitted blade failed. (Das Festlegen der Boot-Reihenfolge für das übermittelte Blade ist fehlgeschlagen).

42 Setting the power control for the submitted blade failed. (Das Festlegen der Netzsteuerung für das übermittelte Blade ist fehlgeschlagen).

43 Setting the max power for the submitted blade failed. (Das Festlegen der maximalen Leistung für das übermittelte Blade ist fehlgeschlagen).

44 Shutting down the submitted blade failed. (Das Herunterfahren des übermittelten Blades ist fehlgeschlagen).

45 Clearing the submitted blade failed. (Das Löschen des übermittelten Blades ist fehlgeschlagen).

46 Getting blade information for the submitted blade failed. (Das Abrufen von Bladeinformationen für das übermittelte Blade ist fehlgeschlagen).

47 Getting blade status for the submitted blade failed. (Das Abrufen des Blade-Status für das übermittelte Blade ist fehlgeschlagen).

48 Getting sensor information for the submitted sensor failed. (Das Abrufen von Sensorinformationen für den übermittelten Sensor ist fehlgeschlagen).

49 Setting the submitted rack name failed. (Das Festlegen des übermittelten Racknamens ist fehlgeschlagen).

50 Getting power supply information for the submitted power supply failed. (Das Abrufen von Netzteilinformationen für das übermittelte Netzteil ist fehlgeschlagen).

51 Getting power supply status for the submitted power supply failed. (Das Abrufen des Netzteilstatus für das übermittelte Netzteil ist fehlgeschlagen).

52 Getting power supply measurements for the submitted power supply failed. (Das Abrufen von Netzteil-Messdaten für das übermittelte Netzteil ist fehlgeschlagen).

53 Setting the Onboard Administrator's UID state failed. (Das Festlegen des UID-Status von Onboard Administrator ist fehlgeschlagen).

54 Getting the Onboard Administrator's status failed. (Das Abrufen des Status von Onboard Administrator ist fehlgeschlagen).

55 Getting the Onboard Administrator's information failed. (Das Abrufen von Onboard Administrator-Informationen ist fehlgeschlagen).

56 Getting fan information for the submitted fan failed. (Das Abrufen von Lüfterinformationen für den übermittelten Lüfter ist fehlgeschlagen).

57 Rebooting the enclosure failed. (Der Neustart des Gehäuses ist fehlgeschlagen).

58 Shutting down the enclosure failed. (Das Herunterfahren des Gehäuses ist fehlgeschlagen).

59 Getting the enclosure information failed. (Das Abrufen von Gehäuseinformationen ist fehlgeschlagen).

60 Getting the enclosure names failed. (Das Abrufen der Gehäusenamen ist fehlgeschlagen).

61 Getting the enclosure status failed. (Das Abrufen des Gehäusestatus ist fehlgeschlagen).

62 Setting the enclosure name failed. (Das Festlegen des Gehäusenamens ist fehlgeschlagen).

63 Setting the enclosure asset tag failed. (Das Festlegen der Gehäusesystemkennung ist fehlgeschlagen).

64 Setting the enclosure time failed. (Das Festlegen der Zeitzone des Gehäuses ist fehlgeschlagen).

65 Setting the enclosure UID failed. (Das Festlegen der Gehäuse-UID ist fehlgeschlagen).

66 Setting the UID for the submitted interconnect failed. (Das Festlegen der UID für das übermittelte Verbindungsmodul ist fehlgeschlagen).

67 Resetting the submitted interconnect failed. (Das Zurücksetzen des übermittelten Verbindungsmoduls ist fehlgeschlagen).

68 Getting interconnect information for the submitted interconnect failed. (Das Abrufen von Verbindungsmodulinformationen für das übermittelte Verbindungsmodul ist fehlgeschlagen).

69 Getting interconnect status for the submitted interconnect failed. (Das Abrufen des Verbindungsmodulstatus für das übermittelte Verbindungsmodul ist fehlgeschlagen).

70 An error occurred while accessing the connected user for the requested blade. (Beim Zugriff auf den verbundenen Benutzer für das angeforderte Blade ist ein Fehler aufgetreten).

71 An error occurred while reading the lockfile for the submitted blade. (Beim Lesen der Sperrdatei für das übermittelte Blade ist ein Fehler aufgetreten).

72 The submitted E-mail address is not valid. (Die übermittelte E-Mail-Adresse ist ungültig).

73 Libem is not able to talk to iLO. (Libem kann nicht mit iLO kommunizieren).

74 Downloading the submitted file failed. (Das Herunterladen der übermittelten Datei ist fehlgeschlagen).

75 The certificate could not be verified. (Das Zertifikat konnte nicht überprüft werden).

76 Could not save the authorization keys. (Der Autorisierungsschlüssel konnte nicht gespeichert werden).

77 The SSH key size is not correct. (Die SSH-Schlüsselgröße ist nicht korrekt).

78 Could not ping the requested url. (Es konnte kein Ping-Signal an den angeforderten URL gesendet werden).

79 Could not generate the CSR. (CSR konnte nicht generiert werden).

80 Could not generate the SSO. (SSO konnte nicht generiert werden).

81 Could not read the fingerprint. (Fingerabdruck konnte nicht gelesen werden).

82 Could not get SSH key. (SSH-Schlüssel konnte nicht abgerufen werden).

83 The field is already enabled. (Das Feld ist bereits aktiviert).

84 The field is already disabled. (Das Feld ist bereits deaktiviert).

85 The system is already in DHCP mode. (Das System befindet sich bereits im DHCP-Modus).

86 The system is currently in static IP mode. (Das System befindet sich derzeit im statischen IP-Modus).

87 Could not clear the system log. (Das Systemprotokoll konnte nicht gelöscht werden).

88 Could not restore the factory settings. (Die Werkseinstellungen konnten nicht wiederhergestellt werden).

89 Could not read the configuration file. (Die Konfigurationsdatei konnte nicht gelesen werden).

90 Could not write to the configuration file. (In die Konfigurationsdatei konnte nicht geschrieben werden).

92 The submitted URL is not valid. (Der übermittelte URL ist ungültig).

93 Could not update the firmware with the submitted image file. (Die Firmware konnte mit der übermittelten Bilddatei nicht aktualisiert werden).

94 Unable to acquire the rack topology. (Die Racktopologie konnte nicht abgerufen werden).

95 Invalid domain. (Ungültige Domäne).

97 Connecting to the blade's iLO failed. (Die Verbindung mit dem iLO des Blades ist fehlgeschlagen).

98 Sending the RIBCL command to the requested blade failed. (Das Senden des RIBCL-Befehls an das angeforderte Blade ist fehlgeschlagen).

99 Could not find the requested element in the RIBCL response. (Das angeforderte Element konnte in der RIBCL-Antwort nicht gefunden werden).

100 Could not find the requested attribute in the RIBCL response. (Das angeforderte Attribut konnte in der RIBCL-Antwort nicht gefunden werden).

101 Could not find the starting boundry in the RIBCL response. (Die Startbegrenzung konnte in der RIBCL-Antwort nicht gefunden werden).

102 Could not find the ending boundry in the RIBCL response. (Die Endbegrenzung konnte in der RIBCL-Antwort nicht gefunden werden).

103 Could not determine the IP address of the management processor for the requested blade. (Die IP-Adresse des Managementprozessors für das angeforderte Blade konnte nicht ermittelt werden).

104 Could not locate a Primary NTP server. (Ein primärer NTP-Server konnte nicht lokalisiert werden).

105 You must set at least one (1) trusted host before enabling trusted hosts. (Sie müssen mindestens einen (1) vertrauenswürdigen Host einstellen, bevor Sie vertrauenswürdige Hosts aktivieren).

107 Could not create the RIBCL request. (RIBCL-Anforderung konnte nicht erstellt werden).

108 This error message should be taken from the soap errorText (varies). (Diese Fehlermeldung sollte aus dem soap errorText bezogen werden, kann variieren).

118 The management processor auto-login feature is not supported. (Die automatische Anmeldefunktion des Managementprozessors wird nicht unterstützt).

119 The maximum number of EBIPA DNS servers has already been reached. (Die maximale Anzahl von EBIPA DNS-Servern wurde bereits erreicht).

120 The starting IP address and Net Mask must be set before enabling EBIPA. (Vor dem Aktivieren von EBIPA muss die Start-IP-Adresse und die Netzmaske eingestellt werden).

121 The LDAP group does not exist. (Die LDAP-Gruppe existiert nicht).

122 The LDAP group already exists. (Die LDAP-Gruppe existiert bereits).

123 The maximum number of LDAP groups has already been reached. (Die maximale Anzahl von LDAP-Gruppen wurde bereit erreicht).

125 Error getting Insight Display information. (Fehler beim Abrufen von Insight Display-Informationen).

126 Error getting Insight Display status. (Fehler beim Abrufen des Insight Display-Status).

127 Error reading the certificate. (Fehler beim Lesen des Zertifikats).

128 Error setting the time zone. (Fehler beim Festlegen der Zeitzone).

129 Error installing the certificate. (Fehler beim Installieren des Zertifikats).

130 Exceeded the maximum number of SSO certificates. (Maximale Anzahl von SSO-Zertifikaten überschritten).

131 The X509 Certificate is not formatted correctly. (Das X509-Zertifikat ist nicht korrekt formatiert).

132 HP SIM station already in trusted list. (HP SIM-Station befindet sich bereits in der vertrauenswürdigen Liste).

133 HP SIM station name not found. (Name der HP SIM-Station nicht gefunden).

134 HP SIM SSO API received a bad parameter. (HP SIM SSO-API hat einen ungültigen Parameter erhalten).

135 The maximum number of HP SIM XE stations already configured. (Die maximale Anzahl von HP SIM XE-Stationen wurde bereits konfiguriert).

136 The maximum number of EBIPA interconnects DNS servers has been reached. (Die maximale Anzahl von EBIPA-Verbindungsmodul-DNS-Servern wurde erreicht).

137 The session could not be created. (Die Sitzung konnte nicht erstellt werden).

138 The session could not be deleted. (Die Sitzung konnte nicht gelöscht werden).

139 Not a valid request while running in standby mode. (Keine gültige Anforderung bei der Ausführung im Standbymodus).

140 Not a valid request while transitioning to active mode. (Keine gültige Anforderung beim Übergang in den aktiven Modus).

141 Not a valid request while running in active mode. (Keine gültige Anforderung bei der Ausführung im aktiven Modus).

142 The maximum number of LDAP certificates already exist. (Die maximale Anzahl von LDAP-Zertifikaten existiert bereits).

143 Could not remove LDAP certificate. (LDAP-Zertifikat existiert bereits).

144 You must configure the directory server and at least one search context before enabling LDAP. (Vor dem Aktivieren von LDAP müssen Sie den Verzeichnisserver und mindestens einen Suchkontext konfigurieren).

145 Could not set the LDAP group description. (Die LDAP-Gruppenbeschreibung konnte nicht eingestellt werden).

146 An error occurred while communicating with the other Onboard Administrator. (Beim Kommunizieren mit dem anderen Onboard Administrator ist ein Fehler aufgetreten).

147 Unable to perform the operation. (Der Vorgang kann nicht durchgeführt werden.) Retry the operation or restart OA. (Vorgang wiederholen oder OA neu starten.) (System Error 147) (Systemfehler 147)

148 The other Onboard Administrator is not present. (Der andere Onboard Administrator ist nicht vorhanden).

149 No redundant Onboard Administrator found. Cannot failover. (Keinen redundanten Onboard Administrator gefunden. Kein Failover möglich.)

150 The user could not be authenticated. (Der Benutzer konnte nicht authentifiziert werden).

151 Invalid parameter for setting blade one time boot. (Ungültiger Parameter beim Einstellen des einmaligen Bootens des Blade).

152 Invalid parameter for setting the blade boot priority. (Ungültiger Parameter beim Einstellen der Blade-Boot-Priorität).

153 A blade boot device can only be listed once. (Das Blade-Boot-Gerät darf nur einmal aufgelistet sein).

154 NTP Poll time must be between 60 and 86400 seconds. (NTP-Abrufzeit muss zwischen 60 und 86400 Sekunden liegen).

155 Could not create new file. (Neue Datei konnte nicht erstellt werden).

156 Could not write the file to the disk. (Die Datei konnte nicht auf den Datenträger geschrieben werden).

157 The submitted image is too big. (Das übermittelte Bild ist zu groß).

158 The submitted image is not a BMP image. (Das übermittelte Bild ist kein BMP-Bild).

159 The submitted image does not have the appropriate dimensions. (Das übermittelte Bild verfügt nicht über die entsprechenden Dimensionen).

160 Non-standard BMP images are not supported. (BMP, die nicht dem Standard entsprechen, werden nicht unterstützt).

161 The specified item was not found. (Das angeforderte Element wurde nicht gefunden).

162 The protocol specified in the URL is not supported. (Das im URL angegebene Protokoll wird nicht unterstützt).

163 The upload to the specified URL failed. (Der Upload an den angegebenen URL ist fehlgeschlagen).

164 The Onboard Administrator did not fail over. (Kein Failover des Onboard Administrators).

165 The blade is in a powered off state. (Das Blade ist ausgeschaltet).

167 The IP manager does not exist. (Der IP-Manager existiert nicht).

168 There is no SSH key installed. (Es ist kein SSH-Schlüssel installiert).

169 There was a problem running the configuration script. (Problem beim Ausführen des Konfigurationsskripts).

170 Missing credentials. (Fehlende Anmeldeinformationen).

171 Caught the SIGSEGV signal. (SIGSEGV-Signal empfangen).

173 No trap receivers were specified. (Keine Trap-Empfänger angegeben).

174 There are no SSH keys installed. (Keine SSH-Schlüssel installiert).

175 There was an error attempting to clear the SSH keys. (Fehler bei dem Versuch, die SSH-Schlüssel zu löschen).

176 The IP address is already listed. (Die IP-Adresse wird bereits aufgelistet).

177 There was an error getting the SSO trust mode. (Fehler beim Aufruf des SSO-Vertrauensmodus).

178 The submitted SSO trust mode is invalid. (Der übermittelte SSO-Vertrauensmodus ist ungültig).

179 The certificate cannot be removed because it does not exist. (Das Zertifikat kann nicht entfernt werden, da es nicht vorhanden ist).

180 The interconnect tray is not present. (Das Verbindungsmodulfach ist nicht vorhanden).

181 The blade is not present. (Das Blade ist nicht vorhanden).

182 Users cannot remove or disable themselves. (Benutzer können sich nicht selbst entfernen oder deaktivieren).

183 Invalid time zone. (Ungültige Zeitzone).

184 Error setting CLP strings. (Fehler beim Festlegen der CLP-Zeichenfolgen).

185 Error getting CLP status. (Fehler beim Anfordern des CLP-Status).

186 Error setting ISMIC info block. (Fehler beim Festlegen des ISMIC-Infoblocks).

187 Error reading ISMIC info block. (Fehler beim Lesen des ISMIC-Infoblocks).

188 Error clearing blade signature. (Fehler beim Löschen der Blade-Signatur).

189 Error setting blade signature. (Fehler beim Festlegen der Blade-Signatur).

190 Request is valid only for server blades. (Anforderung nur für Server Blades gültig).

191 Request is valid only for ProLiant server blades. (Anforderung nur für ProLiant Server Blades gültig).

192 The string entered is not a valid netmask. (Die eingegebene Zeichenfolge ist keine gültige Netzmaske).

193 The string entered is not a valid gateway. (Die eingegebene Zeichenfolge ist kein gültiges Gateway).

194 The string entered for DNS server 1 is not valid. (Die für DNS-Server 1 eingegebene Zeichenfolge ist nicht gültig).

195 The string entered for DNS server 2 is not valid. (Die für DNS-Server 2 eingegebene Zeichenfolge ist nicht gültig).

196 Error trying to remove a nonexistent SSO name. (Fehler beim Entfernen eines nicht vorhandenen SSO-Namens).

197 Error trying to add an SSO name. (Fehler beim Hinzufügen eines SSO-Namens).

198 Invalid SNMP trap community. (Ungültige SNMP-Trap-Community).

201 Could not open the event pipe for reading. (Ereignispipe konnte nicht zum Lesen geöffnet werden).

202 Did not read the proper size for events. (Korrekte Größe für Ereignisse wurde nicht gelesen).

203 Event length mismatch. (Keine Übereinstimmung der Ereignisgröße).

204 The event listener was terminated. (Der Ereignisempfänger wurde beendet).

211 Error obtaining blade power reduction status. (Fehler beim Anfordern des Blade-Stromreduzierungsstatus).

212 Update the other OA firmware to enable this feature. (Aktualisieren Sie die andere OA-Firmware, um diese Funktion zu aktivieren).

213 Dates before 14 June 2006 are not valid. (Datumsangaben vor dem 14. Juni 2006 sind nicht gültig).

214 The certificate exceeds the maximum valid size. (Das Zertifikat überschreitet die maximal gültige Größe).

215 E-Fuse cannot be reset. (E-Sicherung kann nicht zurückgesetzt werden).

216 Firmware update in progress. Login is disabled. (Firmwareaktualisierung im Gange. Anmeldung deaktiviert.)

217 An error occurred while setting the enclosure PDU type. (Beim Festlegen des PDU-Typs des Gehäuses ist ein Fehler aufgetreten).

218 An error occurred while setting the enclosure part number. (Beim Festlegen der Teilenummer des Gehäuses ist ein Fehler aufgetreten).

219 An error occurred while setting the enclosure serial number. (Beim Festlegen der Seriennummer des Gehäuses ist ein Fehler aufgetreten).

220 Cannot set time when NTP is enabled. (Zeit kann nicht festgelegt werden, wenn NTP aktiviert ist).

221 Request is valid only for Itanium/BCS/IPF blades. (Anforderung ist nur für Itanium/BCS/IPF Blades gültig).

222 The Active and Standby Onboard Administrator are not the same hardware build. (Das aktive und das Onboard Administrator-Standby-Modul sind nicht vom gleichen Hardware-Build).

223 The firmware installed on an Onboard Administrator module is incompatible with FirmwareSync. (Die auf einem Onboard Administrator Modul installierte Firmware ist nicht mit der Firmware-Synchronisierung kompatibel).

224 Failed to create firmware image. (Firmware-Image wurde nicht erstellt).

225 The Active and Standby Onboard Administrator have the same firmware version installed. (Im aktiven und im Onboard Administrator-Standby-Modul ist die gleiche Firmwareversion installiert).

226 Upgrade an Onboard Administrator to firmware 2.10 or later to enable this feature. (Aktualisieren Sie ein Onboard Administrator-Modul auf Firmware 2.10 oder höher, um diese Funktion zu aktivieren).

227 The requested user cannot be removed from iLO because it is the only remaining administrator account. (Der angeforderte Benutzer kann nicht von iLO entfernt werden, da es sich bei ihm um das einzige verbleibende Administratorkonto handelt).

228 The requested user cannot be added to iLO because iLO local accounts have been disabled. (Der angeforderte Benutzer kann nicht zu iLO hinzugefügt werden, da lokale iLO-Konten deaktiviert wurden).

229 The requested user cannot be added to iLO because the maximum number of local accounts already exists. (Der angeforderte Benutzer kann nicht zu iLO hinzugefügt werden, da die maximale Anzahl lokaler Konten bereits besteht).

230 One or more of the specified SNMP traps were not already configured on the Onboard Administrator and cannot be removed. (Eine oder mehrere der angegebenen SNMP-Traps waren noch nicht auf Onboard Administrator konfiguriert und können nicht entfernt werden).

231 Reset Factory Defaults in progress. Login disabled. (HP Onboard Administrator wird initialisiert. Anmeldung deaktiviert.)

232 The requested operation is not available on c3000 enclosures. (Der angeforderte Vorgang ist auf c3000 Gehäusen nicht verfügbar).

233 This feature requires the iLO Select Pack License or iLO Advanced Pack License on the server blade when LDAP is enabled on the Onboard Administrator. (Für diese Funktion wird die iLO Select Pack Lizenz oder die iLO Advanced Pack Lizenz auf dem Server Blade benötigt, wenn auf dem Onboard Administrator LDAP aktiviert ist).

234 Invalid characters detected. (Ungültige Zeichen erkannt).

235 HP Onboard Administrator is initializing. Login disabled. (HP Onboard Administrator wird initialisiert. Anmeldung deaktiviert.)

236 Cannot retrieve Onboard Administrator media device array. (Onboard Administrator-Medienkomponenten-Array kann nicht abgerufen werden).

237 The requested device is not ready. (Die angeforderte Komponente ist nicht bereit).

238 Power off or remove the partner blade. (Schalten Sie das Partner-Blade aus oder entfernen Sie es).

239 The current firmware does not support this operation. (Dieser Vorgang wird von der aktuellen Firmware nicht unterstützt).

240 Serial number update requires newer firmware version. (Für die Aktualisierung der Seriennummer wird eine neuere Firmwareversion benötigt).

241 The requested device is not present or no firmware upgrade is required. (Die angeforderte Komponente ist nicht vorhanden oder es ist keine Firmwareaktualisierung erforderlich).

242 The operation cannot be performed on the requested device. (Der Vorgang kann auf der angeforderten Komponente nicht durchgeführt werden).

243 iLO license information cannot be retrieved because iLO XML Reply is disabled. (iLO Lizenzinformationen können nicht abgerufen werden, da ilO XML Reply deaktiviert ist).

244 SSH is disabled on this blade. (SSH ist auf diesem Blade deaktiviert).

245 Disconnect the virtual media applet. (Trennen Sie das virtuelle Medien-Applet).

246 Invalid SNMP Write Community string. (Ungültiger SNMP-Write-Community-String).

247 Invalid SNMP Read Community string. (Ungültiger SNMP-Read-Community-String).

248 Invalid port number. The LDAP server SSL port can be any number between 1 and 65535. (Ungültige Port-Nummer. Der LDAP-Server-SSL-Port kann eine beliebige Nummer zwischen 1 und 65535 sein).

249 Feb 29 was specified but the year is not a leap year. (Es wurde der 29. Februar angegeben, aber dies ist kein Schaltjahr).

250 The CA certificate is invalid. (Das CA-Zertifikat ist ungültig).

251 Exceeded the maximum number of CA certificates. (Maximale Anzahl von SSO-Zertifikaten überschritten).

252 No CA certificates are imported. (Es werden keine CA-Zertifikate importiert).

253 This CA certificate is already imported. (Dieses CA-Zertifikat wurde bereits importiert).

254 A certificate is already mapped to this user. (Diesem Benutzer ist bereits ein Zertifikat zugeordnet).

255 An undocumented error has occurred. Please update your firmware to the latest firmware version if necessary. Contact HP if the problem persists. (Es ist ein nicht dokumentierter Fehler aufgetreten. Aktualisieren Sie die Firmware ggf. auf die neueste Version. Wenden Sie sich an HP, falls das Problem fortbestehen sollte.)

256 This certificate is already mapped to another user. (Dieses Zertifikat ist bereits einem anderen Benutzer zugeordnet).

257 The user certificate could not be verified. (Das Benutzerzertifikat konnte nicht überprüft werden).

258 This operation is not permitted when two-factor authentication is enabled. (Dieser Vorgang ist bei aktivierter 2-Faktor-Authentifizierung nicht zulässig).

260 This operation cannot be performed when AlertMail is disabled. (Dieser Vorgang kann nicht durchgeführt werden, wenn SNMP deaktiviert ist).

261 This operation cannot be performed when the AlertMail settings are not configured. (Dieser Vorgang kann nicht durchgeführt werden, wenn die AlertMail-Einstellungen nicht konfiguriert sind).

262 This operation cannot be performed when SNMP is disabled. (Dieser Vorgang kann nicht durchgeführt werden, wenn SNMP deaktiviert ist).

263 A certificate must be mapped to Administrator or LDAP must be enabled with a configured groups with administrator privilege to enable two-factor authentication. (Dem Administrator muss ein Zertifikat zugeordnet sein oder LDAP muss bei einer konfigurierten Gruppe mit Administratorrechten konfiguriert sein, um die 2-Faktor-Authentifizierung aktivieren zu können).

265 A certificate is not mapped to this user account. (Diesem Benutzerkonto ist kein Zertifikat zugeordnet).

266 Two-factor authentication is in effect. (Die 2-Faktor-Authentifizierung ist wirksam).

267 Two-factor authentication configuration was not changed. (Die Konfiguration der 2-Faktor-Authentifizierung wurde nicht geändert).

268 An iLO image is already staged. (Ein iLO-Image wird bereits eingesetzt).

269 The file was not a proper iLO image for the blade. (Die Datei war kein ordnungsgemäßes iLO-Image für das Blade).

270 The crc32 supplied does not match the provided file. (Der gelieferte crc32 stimmt nicht mit der bereitgestellten Datei überein).

271 Cannot delete the last CA with two-factor authentication enabled. (Die letzte Zertifizierungsstelle kann nicht gelöscht werden, solange die 2-Faktor-Authentifizierung aktiviert ist).

272 The Onboard Administrator cannot communicate with iLO. (Der Onboard Administrator kann nicht mit iLO kommunizieren).

273 An EBIPA configuration error occurred. (Es ist ein EBIPA-Konfigurationsfehler aufgetreten).

274 Link Loss Failover intervals must be between 30 and 86400 seconds. (Failover-Intervalle bei Verbindungsverlust müssen zwischen 30 und 86400 Sekunden liegen).

275 Network speed must be either 10Mbit or 100Mbit. (Die Netzwerkgeschwindigkeit muss zwischen 10 Mb oder 100 Mb betragen).

276 Network duplex setting must be HALF or FULL. (Netzwerk-Duplex-Einstellungen müssen HALB oder VOLL lauten).

277 The password does not conform to password rules. (Das Kennwort entspricht nicht den Kennwortregeln).

278 Invalid minimum password value. (Ungültiger Kennwort-Mindestwert).

279 An firmware image is already staged. (Ein Firmware-Image wird bereits eingesetzt).

280 The provided file was not a proper image. (Die bereitgestellte Datei war nicht das richtige Image).

281 Bad image CRC checksum. (Ungültige Image-CRC-Prüfsumme).

282 Remote system logging must be enabled to perform this operation. (Zum Durchführen dieses Vorgangs muss die Remote-Systemprotokollierung aktiviert sein).

283 Invalid remote port. The port must be a number between 1 and 65535. (Ungültiger Remote-Port. Der Port muss eine Zahl zwischen 1 und 65535 sein.)

284 The remote syslog server address must be configured before enabling remote system logging. (Vor dem Aktivieren der Remote-Systemprotokollierung muss die Serveradresse des Remote-Systemprotokolls konfiguriert werden).

285 Invalid remote server address. (Ungültige Remote-Serveradresse).

286 This setting is already enabled. (Diese Einstellung ist bereits aktiviert).

287 This setting is already disabled. (Diese Einstellung ist bereits deaktiviert).

288 Enclosure IP mode was not enabled because the active Onboard Administrator does not have a static IPv4 address. (Der IP-Modus des Gehäuses wurde nicht aktiviert, da das aktive Onboard Administrator-Modul über keine statische IPv4-Adresse verfügt).

289 This feature is not available for this Onboard Administrator. (Diese Funktion ist für diesen Onboard Administrator nicht verfügbar).

290 Request to enable DHCP addressing on the active Onboard Administrator is denied because Enclosure IP Mode is enabled. (Anforderung zum Aktivieren der DHCP-Adressierung auf dem aktiven Onboard Administrator-Modul abgelehnt, da der IP-Modus des Gehäuses aktiviert ist).

291 The value provided is not proper base64. (Der bereitgestellte Wert ist nicht base64).

292 The firmware image provided is an older version than the current firmware. Onboard Administrator settings cannot be preserved. (Das bereitgestellte Firmware-Image ist eine ältere Version als die aktuelle Firmware. Die Einstellungen von Onboard Administrator können nicht beigehalten werden.)

293 The file provided is not a valid Onboard Administrator firmware image. (Die bereitgestellte Datei ist kein gültiges Onboard Administrator-Firmware-Image).

294 There are no USB keys connected to the enclosure. (Am Gehäuse sind keine USB-Schlüssel angeschlossen).

295 No valid firmware images found on USB key. (Keine gültigen Firmware-Images auf dem USB-Schlüssel gefunden).

296 No configuration scripts found on USB key. (Keine Konfigurationsskripts auf dem USB-Schlüssel gefunden).

297 I/O error on USB key. (I/O-Fehler auf dem USB-Schlüssel).

298 Badly formatted USB file URL. (Ungültig formatierter URL der USB-Datei).

299 Permission problems when accessing USB media. (Berechtigungsprobleme beim Zugriff auf USB-Medien).

300 Error uploading to USB media. (Fehler beim Hochladen auf USB-Medien).

301 An invalid number of GUIDs was passed to the Onboard Administrator. (Eine ungültige Anzahl von GUIDs wurde dem Onboard Administrator übergeben).

302 URL flash image for microcode download not available. (URL-Flash-Image für Mikrocode-Download nicht verfügbar).

303 Invalid session timeout. (Ungültige Sitzungszeitüberschreitung).

304 Invalid watts value. (Ungültiger Wert für Watt).

305 Failed to store change for power cap. (Änderung für Stromobergrenze wurde nicht gespeichert).

306 Enclosure Dynamic Power Cap feature is not allowed. (Die Gehäusefunktion der dynamischen Stromobergrenze ist nicht zulässig).

307 Wrong number of bays specified for enclosure while setting capping bays to exclude. (Beim Festlegen der Einschübe mit Obergrenze wurde die falsche Anzahl von Einschüben angegeben).

308 The number of bays opted out exceeds the maximum allowed. (Die Anzahl der ausgeschlossenen Einschübe überschreitet den zulässigen Höchstwert).

309 Enclosure Dynamic Power Cap feature is not allowed. (Die Gehäusefunktion der dynamischen Stromobergrenze ist nicht zulässig).

310 Enclosure Dynamic Power Cap is set. (Die dynamische Stromobergrenze des Gehäuses ist festgelegt).

311 Enclosure Dynamic Power Cap is not set. Cannot confirm that device tray meets minimum firmware version required. (Keine dynamische Stromobergrenze des Gehäuses ist festgelegt. Es kann nicht bestätigt werden, ob das Komponentenfach der erforderlichen Mindestversion der Firmware entspricht).

312 Enclosure Dynamic Power Cap not set. Device tray fails to meet the minimum required firmware version. (Keine dynamische Stromobergrenze des Gehäuses festgelegt. Das Komponentenfach erfüllt nicht die erforderliche Mindestversion der Firmware.)

313 The requested cap is outside the allowable range of Enclosure Dynamic Power Cap values. (Die angeforderte Obergrenze liegt außerhalb des zulässigen Bereichs der Werte für die dynamische Obergrenze des Gehäuses).

314 Server Power Reduction cannot currently be enabled. Enclosure Dynamic Power Cap is not allowed. (Die Stromreduzierung des Servers kann derzeit nicht aktiviert werden. Es ist keine dynamische Stromobergrenze für das Gehäuse zulässig.)

315 No valid ISO images found on USB key. (Keine gültigen ISO-Images auf dem USB-Schlüssel gefunden).

316 Bay privileges cannot be revoked for Administrators with OA permission. (Einschubsberechtigungen können für Administratoren mit OA-Berechtigung nicht aufgehoben werden).

317 Invalid DNS hostname. (Ungültiger DNS-Hostname).

318 Factory defaults cannot be restored because the enclosure is in VC mode. (Werkseinstellungen können nicht wiederhergestellt werden, da sich das Gehäuse im VC-Modus befindet).

319 The string entered is not a valid IPv6 address. (Die eingegebene Zeichenfolge ist keine gültige IPv6-Adresse).

320 IPv6 static address already exists. (Statische IPv6-Adresse bereits vorhanden).

321 IPv6 static address not found. (Statische IPv6-Adresse nicht gefunden).

322 Unable to add. (Hinzufügen nicht möglich).

323 Invalid SMTP server. (Ungültiger NTP-Server).

324 Invalid SNMP Trap receiver. (Ungültiger SNMP-Trap-Empfänger).

325 Invalid NTP server. (Ungültiger NTP-Server).

326 Invalid EBIPA configuration. Multiple subnets were detected. (Ungültige EBIPA-Konfiguration. Es wurden mehrere Subnetze erkannt.)

327 Specified VLAN ID does not exist. (Angegebene VLAN ID nicht vorhanden).

328 Cannot delete the default VLAN ID. (Die Standard-VLAN-ID kann nicht gelöscht werden).

329 Maximum VLAN entries reached. (Höchstzahl von VLAN-Einträgen erreicht).

330 Duplicated VLAN ID. (Doppelte VLAN-ID).

331 Specified VLAN ID is invalid. (Die angegebene VLAN-ID ist ungültig).

332 Operation partially successful. (Vorgang teilweise erfolgreich).

333 Duplicated VLAN name. (Doppelter VLAN-Name).

334 A pending command already exists. (Ein anstehender Befehl ist bereits vorhanden).

337 The remote syslog server address cannot be cleared while remote logging is enabled. (The Serveradresse der Remote-Systemprotokollierung kann nicht gelöscht werden, solange die Remote-Protokollierung aktiviert ist).

338 Invalid search context number. (Ungültige Suchkontextnummer).

339 Not on the same VLAN ID domain. (Nicht auf der gleichen VLAN-ID-Domäne).

340 This command is not valid for auxiliary blades. (Dieser Befehl ist für Zusatz-Blades nicht gültig).

341 No LDAP groups currently exist. (Derzeit sind keine LDAP-Gruppen vorhanden).

342 The requested Derated Circuit Capacity is outside the allowable range of values for this enclosure. (Die angeforderte herabgesetzte Schaltkreiskapazität liegt außerhalb des zulässigen Bereichs von Werten für dieses Gehäuse).

343 The requested Rated Circuit Capacity is outside the allowable range of values for this enclosure. (Die angeforderte Nennkapazität des Schaltkreises liegt außerhalb des zulässigen Bereichs von Werten für dieses Gehäuse).

344 The requested cap is greater than the requested Derated Circuit Capacity. (Die angeforderte Obergrenze ist höher als die angeforderte herabgesetzte Schaltkreiskapazität).

345 The requested Derated Circuit Capacity is greater than the requested Rated Circuit Capacity. (Die angeforderte herabgesetzte Schaltkreiskapazität ist größer als die angeforderte Nennkapazität des Schaltkreises).

346 The requested set of bays to exclude cause the cap to be outside the allowable range. (Der angeforderte Satz auszuschließender Einschübe hat zur Folge, dass die Obergrenze außerhalb des zulässigen Bereichs liegt).

347 The requested set of bays to exclude cause the Derated Circuit Capacity to be outside the allowable range. (Der angeforderte Satz auszuschließender Einschübe hat zur Folge, dass die herabgesetzte Schaltkreiskapazität außerhalb des zulässigen Bereichs liegt).

348 The requested set of bays to exclude cause the Rated Circuit Capacity to be outside the allowable range. (Der angeforderte Satz auszuschließender Einschübe hat zur Folge, dass die herabgesetzte Nennkapazität des Schaltkreises außerhalb des zulässigen Bereichs liegt).

353 IPv6 is currently disabled. Cannot download certificate from the specified address. (IPv6 derzeit deaktiviert. Zertifikat kann nicht von der angegebenen Adresse heruntergeladen werden.)

354 The date cannot be set to a date in the past. (Für das Datum kann kein vergangenes Datum eingestellt werden.)

356 The setting cannot be cleared while LDAP is enabled. (Die Einstellung kann nicht gelöscht werden, während LDAP aktiviert ist.)

357 URB reporting using HTTP(S) cannot be enabled until an HTTP(S) endpoint has been configured. (URB-Berichterstellung mittels HTTP(S) kann erst aktiviert werden, nachdem ein HTTP(S)-Endpunkt konfiguriert wurde.)

358 URB reporting using SMTP cannot be enabled until an SMTP server and mailbox have been configured. (URB-Berichterstellung mittels SMTP kann erst aktiviert werden, nachdem ein SMTP-Server und eine Mailbox konfiguriert wurden.)

359 URB reporting using SMTP and HTTP(S) cannot be enabled until an HTTP(S) and SMTP settings have been configured. (URB-Berichterstellung mittels SMTP und HTTP(S) kann erst aktiviert werden, nachdem HTTP(S)- und SMTP-Einstellungen konfiguriert wurden.)

360 Warning: Not all VC-Enet modules are on the same VLAN ID. (Warnung: Nicht alle VC-Enet-Module befinden sich auf der gleichen VLAN-ID.)

361 File doesn't exist. (Datei nicht vorhanden.)

362 This operation cannot be performed when AlertMail is disabled. (Dieser Vorgang kann nicht durchgeführt werden, wenn AlertMail aktiviert ist).

363 Setting SolutionsId failed. (Setzen von SolutionsID fehlgeschlagen).

364 SolutionsId must be an 8-byte hex string, between 0000000000000000 and FFFFFFFFFFFFFFFF. (SolutionsId muss eine 8-Byte hexadezimale Zeichenfolge zwischen 0000000000000000 und FFFFFFFFFFFFFFFF sein.)

365 Failed Remote Support registration. (Remote-Support-Registrierung fehlgeschlagen).

366 Failed Remote Support un-registration. (Aufheben der Remote-Support-Registrierung fehlgeschlagen).

367 Failed Remote Support restore registration. (Remote-Support-Wiederherstellungs-Registrierung fehlgeschlagen).

368 Failed to send Remote Support message (Hint: Check the Remote Support proxy and endpoint URL. Use SET REMOTE_SUPPORT PROXY to configure and re-try.) (Senden der Remote Support-Nachricht fehlgeschlagen (Tip: Überprüfen Sie den Remote Support-Proxy und -Endpunkt-URL. Verwenden Sie zur Konfigurierung SET REMOTE_SUPPORT PROXY und wiederholen Sie den Vorgang.)

369 Failed to set Remote Support interval. Valid interval is 0 to 60 (days). (Das Remote-Support-Intervall wurde nicht festgelegt. Ein gültiges Intervall ist 0 bis 60 (Tage)).

370 You must configure the directory server and SSL port before testing LDAP. (Vor dem Testen von LDAP müssen Sie den Verzeichnisserver und den SSL-Port konfigurieren.)

371 The string contains an invalid character. (Die Zeichenfolge enthält ein ungültiges Zeichen.)

372 This operation cannot be performed when Remote Support is disabled. (Dieser Vorgang kann nicht durchgeführt werden, wenn Remote-Support deaktiviert ist).

373 Cannot set Maintenance Mode Timeout. Value should be between 5 minutes and 2 weeks. (Zeitlimit des Wartungsmodus kann nicht festgelegt werden. Der Wert sollte zwischen 5 Minuten und 2 Wochen liegen.)

374 Insert eRs error here. (eRS-Fehler hier einfügen.)

375 The string entered is not a valid LDAP server. A LDAP server must be a IP address or DNS name. (Die eingegebene Zeichenfolge ist kein gültiger LDAP-Server. Ein LDAP-Server muss eine IP-Adresse oder ein DNS-Name sein.)

376 Unable to perform the operation. (Der Vorgang kann nicht durchgeführt werden.) Retry the operation or restart OA. (Vorgang wiederholen oder OA neu starten.) (System Error 376) (Systemfehler 376)

377 The HP Passport credentials provided are invalid. (Die angegebenen HP Passport-Anmeldedaten sind ungültig.)

378 This system is already registered. (Dieses System ist bereits registriert.)

379 Please disable Remote Support before performing this action. (Bitte deaktivieren Sie Remote-Support, bevor Sie diese Aktion durchführen.)

380 Transaction UUID is mismatched. (Transaktions-UUID ist unstimmig.)

381 Unable to download ilo flash image from the url provided. Supported protocols are http, https, tftp and ftp. (iLO Flash-Image kann nicht über den angegebenen URL heruntergeladen werden. Unterstützte Protokolle sind http, https, tftp und ftp.)

382 The Onboard Administrator is still initializing. Please try your request again later. (Der Onboard Administrator wird immer noch initialisiert. Wiederholen Sie später Ihre Anforderung.)

383 Failed to send Remote Support message. (Remote-Support-Meldung wurde nicht gesendet.) Please make sure DNS is enabled and verify Insight Remote Support host and port information. (Stellen Sie sicher, dass der DNS aktiviert ist, und überprüfen Sie die Host- und Port-Informationen von Insight Remote Support.)

384 Failed to resolve HP Insight Remote Support hosting server. (Der Hostserver von HP Insight Remote Support wurde nicht aufgelöst.) Please verify DNS settings and Insight Remote Support host and port information. (Überprüfen Sie die DNS-Einstellungen und die Host- und Port-Informationen von Insight Remote Support.)

385 Transmission to the HP Insight Remote Support receiver was unsuccessful. (Die Übertragung zum HP Insight Remote Support-Empfänger war nicht erfolgreich.) Please check connectivity between the OA and the Insight Remote Support receiver. (Überprüfen Sie die Verbindung zum OA und zum Insight Remote Support-Host.)

389 This action cannot be performed in FIPS MODE ON/DEBUG. (Diese Aktion kann in FIPS MODE ON/DEBUG nicht durchgeführt werden.)

391 No Variable Name-Value pairs are provided for substitution. (Es wurden keine Variablenname-Wert-Paare als Ersatz bereitgestellt.)

392 Attempted to substitute more than 25 variables. (Es wurde versucht, mehr als 25 Variablen zu ersetzen.)

395 Trying to substitute the same variable twice. (Es wurde versucht, die gleiche Variable zweimal zu ersetzen.)

396 String_list searchFlag out of range. (Bereichsüberschreitung des String_list searchFlag.)

397 No variable names are passed in for searching. (Es wurden keine zu suchenden Variablennamen übergeben.)

398 No variable values are passed in for searching. (Es wurden keine zu suchenden Variablenwerte übergeben.)

401 Enclosure Firmware Management is currently disabled. (Das Enclosure Firmware Management ist derzeit deaktiviert).

402 The Enclosure Firmware Management ISO URL is not set. (Kein URL für das ISO-Image des Enclosure Firmware Management festgelegt).

403 The operation cannot be performed while Enclosure Firmware Management is running. (Der Vorgang kann nicht durchgeführt werden, während das Enclosure Firmware Management ausgeführt wird.)

404 Unable to mount ISO or validate version information. (ISO-Image kann nicht bereitgestellt werden oder Versionsinformationen können nicht validiert werden.)

Check URL and validate ISO is available from URL entered. (Überprüfen Sie den URL und stellen Sie sicher, dass das ISO-Image über den eingegebenen URL verfügbar ist.)

405 Unable to open firmware log. (Firmware-Protokoll kann nicht geöffnet werden.)

406 The blade's firmware has not been discovered. (Die Blade-Firmware wurde nicht ermittelt.)

407 An error occurred while reading the firmware log. (Beim Lesen des Firmware-Protokolls ist ein Fehler aufgetreten.)

408 Enclosure Firmware Management is not supported by this device type. (Das Enclosure Firmware Management wird von diesem Gerätetyp nicht unterstützt).

409 Firmware ISO image is in use, changing url is not allowed. (Das Firmware-ISO-Image wird derzeit verwendet. Eine Änderung der URL ist nicht zulässig.)

410 Blade must be powered off before starting Enclosure Firmware Management. (Blade muss vor dem Starten des Enclosure Firmware Management ausgeschaltet werden.)

411 Unable to change passwords for any LDAP or HPSIM users. (Die Kennwörter für LDAP- oder HPSIM-Benutzer können nicht geändert werden.)

412 Enclosure Firmware Management is not available. To use this feature, it needs to be unlocked. (Das Enclosure Firmware Management ist nicht verfügbar. Diese Funktion muss zum Verwenden entsperrt werden.)

413 Enclosure Firmware Management is not supported on the Active OA hardware present. (Das Enclosure Firmware Management wird auf der vorhandenen Hardware des aktiven OA-Moduls nicht unterstützt.)

414 Could not persist firmware management log. (Firmware-Management-Protokoll konnte nicht beibehalten werden.)

415 When in FIPS MODE ON/DEBUG, the password length must be between 8 and 40 characters. (In FIPS MODE ON/DEBUG muss die Länge von Kennwörtern zwischen 8 und 40 Zeichen betragen.)

416 When in FIPS MODE ON/DEBUG, strict passwords must be enabled. (In FIPS MODE ON/DEBUG müssen strenge Kennwörter aktiviert sein.)

417 Certificate hash algorithm is not supported. (Zertifikat-Hash-Algorithmus nicht unterstützt.) See OA syslog for more information. (Weitere Informationen finden Sie im OA-Systemprotokoll.)

418 Downgrade is not allowed in FIPS mode ON/DEBUG. (Eine Herabstufung ist im FIPS-Modus ON/DEBUG nicht zulässig.) Please set FIPS mode to OFF and retry the operation. (Stellen Sie für den FIPS-Modus OFF ein und wiederholen Sie den Vorgang.)

419 Could not persist firmware management log. (Firmware-Management-Protokoll konnte nicht beibehalten werden.)

427 E-Keying busy. (E-Keying belegt.)

428 Error getting CLP strings. (Fehler beim Abrufen der CLP-Zeichenfolgen).

431 Enclosure Firmware Management is not ready, please try again in a few minutes. (Das Enclosure Firmware Management ist nicht bereit. Wiederholen Sie den Vorgang in einigen Minuten.)

434 PIN Protection cannot be disabled in FIPS Mode. (PIN-Schutz kann im FIPS-Modus nicht deaktiviert werden.)

435 Cannot restore the factory defaults while in FIPS mode. (Die Standard-Werkseinstellungen können im FIPS-Modus nicht wiederhergestellt werden.)

437 Bad EBIPAv6 device. (Fehlerhaftes EBIPAv6-Gerät.)

438 An EBIPAv6 configuration error occurred. (Es ist ein EBIPA-Konfigurationsfehler aufgetreten). Extended information is available as a bitcode reason code. (Erweiterte Informationen sind in Form eines Bitcode-Ursachencodes verfügbar.)

439 Invalid hash algorithm. (Ungültiger Algorithmus.) The hash algorithm must be one of: SHA1, SHA-224, SHA-256, SHA-384, or SHA-512. (Der Hash-Algorithmus muss einer der Folgenden sein: SHA1, SHA-224, SHA-256, SHA-384 oder SHA-512.)

440 You must set a new pin code before unlocking the LCD buttons. (Sie müssen vor Aufheben der LCD-Tastensperre einen neuen PIN-Code eingeben.)

441 The requested operation cannot be completed during a firmware update. (Der angeforderte Vorgang kann während einer Firmwareaktualisierung nicht durchgeführt werden.)

442 This enclosure is incapable of performing a reset on a non-redundant Onboard Administrator. (Dieses Gehäuse kann einen nicht-redundanten Onboard Administrator nicht zurücksetzen.)

444 Power cap configuration locked due to active group management. (Konfiguration der Stromobergrenze aufgrund aktiver Gruppenverwaltung gesperrt.)

REMOTE SUPPORT TIER2

445 HP Remote Support receiver temporarily unavailable. (HP Remote Support-Empfänger vorübergehend nicht verfügbar.) Please retry later. (Bitte später erneut versuchen.)

446 Unregistration request was not processed successfully by the HP Remote Support receiver. (Anforderung zum Aufheben der Registrierung wurde vom HP Remote Support-Empfänger nicht erfolgreich verarbeitet.) Remote Support has been disabled locally. (Remote Support wurde lokal deaktiviert.) No service events or data collections will be sent until this device has been re-registered. (Es werden erst dann wieder Dienstereignisse und Datenerfassungen gesendet, nachdem dieses Gerät erneut registriert wurde.)

447 Authentication error. (Authentifizierungsfehler.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

449 Missing device identifiers. (Fehlende Gerätekennungen.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

449 Corrupt device identifiers. (Beschädigte Gerätekennungen.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

450 Insufficient device identifier information. (Nicht ausreichende Geräte-Kennungsinformationen.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

451 Invalid device identifier information. (Ungültige Geräte-Kennungsinformationen.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

452 Stale device identifiers. (Veraltete Gerätekennungen.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

453 Missing GDID. (Fehlende GDID.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

454 Corrupt GDID. (Beschädigte GDID.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

455 Missing registration token. (Fehlendes Registrierungs-Token.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

456 Corrupt registration token. (Beschädigtes Registrierungs-Token.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

457 Expired registration token. (Abgelaufenes Registrierungs-Token.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

458 Invalid HP Passport credentials. (Ungültige HP Passport Anmeldeinformationen.) Please verify and enter valid HP Passport account credentials. (Überprüfen Sie die Anmeldeinformationen des HP Passport-Kontos und machen Sie gültige Angaben.)

459 Device is already registered. (Gerät bereits registriert.) Please delete the device from Insight Remote Support user interface and retry registration. (Löschen Sie den Dienst von der Insight Remote Support-Benutzeroberfläche, und wiederholen Sie den Registrierungsvorgang.)

460 Unknown device. (Unbekanntes Gerät.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

461 Insufficient registration data. (Unzureichende Registrierungsdaten.) Wiederholen Sie den Registrierungsvorgang.

462 Missing SOAP header. (Fehlender SOAP-Header.) Please retry you last step. (Wiederholen Sie den letzten Schritt.) If error persists and device is currently registered, unregister and re-register device. (Wenn der Fehler fortbesteht und das Gerät derzeit registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

463 Missing GDID. (Fehlende GDID.) Please retry your last step. (Wiederholen Sie den letzten Schritt.) If error persists and device is currently registered, unregister and re-register device. (Wenn der Fehler fortbesteht und das Gerät derzeit registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

464 Missing GDID. (Fehlende GDID.) Wiederholen Sie den letzten Schritt. If error persists and device is currently registered, unregister and re-register device. (Wenn der Fehler fortbesteht und das Gerät derzeit registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

465 Missing data package. (Fehlendes Datenpaket.) Please retry your last step. (Wiederholen Sie den letzten Schritt.) If error persists and device is currently registered, unregister and re-register device. (Wenn der Fehler fortbesteht und das Gerät derzeit registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

466 Data Package validation failed. (Datenpaket-Überprüfung fehlgeschlagen.) Please retry your last step. (Wiederholen Sie den letzten Schritt.) If error persists and device is currently registered, unregister and re-register device. (Wenn der Fehler fortbesteht und das Gerät derzeit registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

467 HP Passport password must be changed or reset. (HP Password muss geändert oder zurückgesetzt werden.) Please attempt to register again after correcting the HP Passport account issue. (Wiederholen Sie die Registrierung, nachdem das Problem mit dem HP Passport-Konto behoben wurde.)

468 Expired HP Passport credentials. (Abgelaufene HP Passport-Anmeldeinformationen.) Please attempt to register again after correcting the HP Passport account issue. (Wiederholen Sie die Registrierung, nachdem das Problem mit dem HP Passport-Konto behoben wurde.)

469 HP Passport account locked out. (HP Passport-Konto gesperrt.) Please attempt to register again after correcting the HP Passport account issue. (Wiederholen Sie die Registrierung, nachdem das Problem mit dem HP Passport-Konto behoben wurde.)

470 GUID and device identifiers do not match. (GUID und Gerätekennungen stimmen nicht überein.) If error persists and device is not currently registered, unregister and re-register device. (Wenn der

Fehler fortbesteht und das Gerät derzeit nicht registriert ist, heben Sie die Registrierung auf, und registrieren Sie das Gerät erneut.)

471 Device is not registered. (Gerät nicht registriert.) Remote Support registration has been disabled locally on this device. (Die Remote Support-Registrierung wurde lokal auf diesem Gerät deaktiviert.) No service events or data collections will be sent until this device has been re-registered. (Es werden erst dann wieder Dienstereignisse und Datenerfassungen gesendet, nachdem dieses Gerät erneut registriert wurde.)

472 Deleted device. (Gelöschtes Gerät.) This device has been previously deleted from the Insight Remote Support user interface. (Dieses Gerät wurde zuvor von der Insight Remote Support-Benutzeroberfläche gelöscht.) Please unregister and re-register device. (Heben Sie die Registrierung des Geräts auf, und registrieren Sie es wieder.)

473 Unhandled error. (Nicht behandelter Fehler.)

474 Failed to connect to HP Insight Remote Support direct connect web service. (Verbindung zu dem Direct Connect-Webdienst von HP Insight Remote Support fehlgeschlagen.) Please verify DNS settings, proxy settings and connectivity. (Überprüfen Sie die DNS-Einstellungen, Proxyeinstellungen und Konnektivität.)

475 Dynamic DNS is not enabled. (Dynamische DNS nicht aktiviert.)

476 Invalid SNMP Engine ID. (Ungültige SNMP-Modul-ID). The Engine ID must start with '0x' followed by an even number of up to 64 hexadecimal digits. (Die Modul-ID muss mit „0x“ beginnen, gefolgt von einer geraden Zahl aus bis zu 64 hexadezimalen Ziffern.)

477 Invalid Authentication Protocol. (Ungültiges Authentifizierungsprotokoll.)

478 Invalid Authentication Password, must contain 8 to 40 printable characters. (Ungültiges Authentifizierungskennwort; es muss 8 bis 40 ausdruckbare Zeichen enthalten.)

479 Invalid Privacy Protocol. (Ungültiges Datenschutzprotokoll.)

480 Invalid Privacy Password, must contain 8 to 40 printable characters. (Ungültiges Datenschutzkennwort; es muss 8 bis 40 ausdruckbare Zeichen enthalten.)

481 Duplicate user, a SNMP user by this name and engine id already exists. (Doppelter Benutzer, ein SNMP-Benutzer mit diesem Namen und dieser Modul-ID ist bereits vorhanden.)

482 Invalid minimal security setting. (Ungültige minimale Sicherheitseinstellung.)

483 Invalid security setting. (Ungültige Sicherheitseinstellung.)

484 Selected algorithm cannot be used while FIPS mode is enabled. (Ausgewählter Algorithmus kann nicht verwendet werden, während der FIPS-Modus aktiviert ist.)

485 A user with read-write access cannot be created while FIPS mode is enabled. (Ein Benutzer mit Lese-Schreib-Zugriff kann nicht erstellt werden, während der FIPS-Modus aktiviert ist.)

486 You cannot use a remote engine id with a trap. (Mit einem Trap kann keine Remote-Modul-ID verwendet werden.)

487 You cannot use the local engine id with an inform. (Mit einem INFORM kann keine lokale Modul-ID verwendet werden.)

489 Error adding the language pack. (Fehler beim Hinzufügen eines Sprachpakets.)

490 Error removing the language pack. (Fehler beim Entfernen eines Sprachpakets.)

491 The file provided is not a valid Onboard Administrator language pack image. (Die bereitgestellte Datei ist kein gültiges Onboard Administrator-Firmware-Image.)

492 Error removing the English language pack. (Fehler beim Entfernen des englischen Sprachpakets.)

493 The language support pack is not installed. (Das Sprachen-Unterstützungspaket ist nicht installiert.)

494 The submitted file is not a valid SSH key. (Die unterstützte Datei ist kein gültiger SSH-Schlüssel.)

499 The firmware image provided doesn't meet the VC Minimum Firmware Version requirement. (Das Firmware-Image entspricht nicht der erforderlichen minimalen VC-Firmwareversion.) Check the OA Syslog for more details. (Weitere Einzelheiten finden Sie im OA-Systemprotokoll.)

500 The action did not complete successfully. (Die Aktion wurde nicht erfolgreich durchgeführt.)

502 Invalid response. (Ungültige Antwort.) No connection or network busy. (Keine Verbindung oder Netzwerk belegt.)

503 Web server busy or in service. (Webserver belegt oder wird gewartet.)

510 Remote Support services are provided by other solution. (Remote Support-Dienste werden durch eine andere Lösung bereitgestellt.)

511 DHCP-Supplied Domain Name cannot be disabled when the user-supplied domain name is not set. (Der vom DHCP bereitgestellte Domänenname kann nicht deaktiviert werden, wenn kein vom Benutzer bereitgestellter Domänenname festgelegt wurde.)

512 The text must contain at least one visible character. (Der Text muss mindestens ein sichtbares Zeichen enthalten.)

514 User ID is a required filed. (Die Benutzer-ID ist ein erforderliches Feld.) Please retry registration. (Wiederholen Sie den Registrierungsvorgang.)

515 The user must have an active authenticated session. (Der Benutzer muss über eine aktive authentifizierte Sitzung verfügen.) Please retry registration. (Wiederholen Sie den Registrierungsvorgang.)

516 HP Passport system failure occurred. (Das HP Passport-System ist ausgefallen.) A problem has been detected in the HP Passport system. (Im HP Passport System wurde ein Problem festgestellt.) Please retry later. (Bitte später erneut versuchen.)

517 The session token is invalid due to any of the following reasons: failed decoding, token is null or empty, userId is empty or session start value is not a number. (Das Sitzungs-Token ist aus einem der folgenden Gründe ungültig: fehlgeschlagene Decodierung, Token ist null oder leer, userID ist leer oder Sitzungs-Startwert ist keine Zahl.) Please retry registration. (Wiederholen Sie den Registrierungsvorgang.)

518 Password required. (Kennwort erforderlich.) Please retry registration. (Wiederholen Sie den Registrierungsvorgang.)

519 HP Passport user ID is invalid. (Die HP Passport-Benutzer-ID ist ungültig.) Please retry registration with a valid user ID. (Wiederholen Sie die Registrierung mit einer gültigen Benutzer-ID.)

520 HP Passport account is locked out due to excessive login authentication failure. (Das HP Passport-Konto ist aufgrund einer übermäßigen Anzahl fehlgeschlagener Anmeldeauthentifizierungen gesperrt.) Please reset your password and retry registration. (Setzen Sie Ihr Kennwort zurück, und wiederholen Sie die Registrierung.)

521 User has reached half the maximum allowed HP Passport login authentication failures. (Der Benutzer hat die Hälfte der zulässigen Anzahl fehlgeschlagener HP Passport-Anmeldeauthentifizierungen erreicht.) Please verify your username and password are correct and retry registration. (Überprüfen Sie Ihren Benutzernamen und Ihr Kennwort auf deren Richtigkeit, und wiederholen Sie die Registrierung.)

522 HP Passport password has expired. (Das HP Password-Kennwort ist abgelaufen.) Please update your password and retry registration. (Aktualisieren Sie Ihr Kennwort, und wiederholen Sie die Registrierung.)

523 User has at least one of the HP Passport required on-line identity elements missing. (Dem Benutzer fehlt mindestens eines der erforderlichen Elemente der HP Passport-Online-Identität.) Please update your HP Passport profile and retry registration. (Aktualisieren Sie Ihr HP Passport-Profil und wiederholen Sie die Registrierung.)

524 HP Passport Security Q and A is not compliant; the user must enter a new security Q and A upon login. (Die HP Passport-Sicherheitsfrage und -antwort sind unstimmig. Der Benutzer muss bei der Anmeldung eine neue Sicherheitsfrage und -antwort eingeben.) Please update your HP Passport security Q and A and retry registration. (Aktualisieren Sie die HP Passport-Sicherheitsfrage und -antwort, und wiederholen Sie die Registrierung.)

525 HP Passport password entered is incorrect. (Das eingegebene HP Passport-Kennwort ist inkorrekt.) Please retry registration using the correct password. (Wiederhole Sie die Registrierung mit dem korrekten Kennwort.)

526 HP Passport user has been added to a group. (HP Passport-Benutzer wurde einer Gruppe hinzugefügt.) Please reset your password and retry registration. (Setzen Sie Ihr Kennwort zurück, und wiederholen Sie die Registrierung.)

527 User must enter an HP Passport security Q and A and change password. (Der Benutzer muss eine HP Passport-Sicherheitsfrage und -antwort eingeben und das Kennwort ändern.) Please update your security Q and A, update your password, and retry registration. (Aktualisieren Sie Ihre Sicherheitsfrage und -antwort, aktualisieren Sie ihr Kennwort und wiederholen Sie die Registrierung.)

528 Protocol error occurred while communicating with the HP Insight Remote Support receiver. (Protokollfehler während der Kommunikation mit dem HP Insight Remote Support-Empfänger.)

529 Failed to resolve proxy. (Proxy wurde nicht aufgelöst.) Please verify DNS settings, proxy settings and connectivity. (Überprüfen Sie die DNS-Einstellungen, Proxyeinstellungen und Konnektivität.)

530 Failed to connect to the HP Insight Remote Support hosting server. (Verbindung zu dem Hostserver von HP Insight Remote Support fehlgeschlagen.) Please verify Insight Remote Support host and port information. (Überprüfen Sie die Host- und Port-Informationen von Insight Remote Support.)

531 Failed to connect to HP Insight Remote Support direct connect web service. (Verbindung zu dem Direct Connect-Webdienst von HP Insight Remote Support fehlgeschlagen.) Please verify DNS settings, proxy settings and connectivity. (Überprüfen Sie die DNS-Einstellungen, Proxyeinstellungen und Konnektivität.)

532 HP Remote Support receiver protocol error. (Fehler des HP Remote Support-Empfängerprotokolls.)

533 The setting cannot be cleared when user domain name is enabled. (Diese Einstellung kann nicht gelöscht werden, wenn der Benutzerdomänenname aktiviert ist.)

534 The operation cannot be performed while Enclosure Firmware Management is enabled. (Der Vorgang kann nicht durchgeführt werden, während das Enclosure Firmware Management aktiviert ist.)

535 Invalid SNMP Engine ID string. (Ungültiger SNMP-Modul-ID-String). The Engine ID string must contain 1 to 27 printable characters. (Der Modul-ID-String muss 1 bis 27 Zeichen enthalten.)

536 The password is too short. (Das Kennwort ist zu kurz.)

537 The password is too long. (Das Kennwort ist zu lang.)

538 Error installing the certificate. (Fehler beim Installieren des Zertifikats).

539 Enclosure IP mode requires the active Onboard Administrator to have a static IPv4 address or a static IPv6 address. (Für den „Enclosure IP Mode“ (Gehäuse-IP-Modus) muss der aktive Onboard Administrator über eine statische IPv4- oder eine statische IPv6-Adresse verfügen.) If IPv6 is not enabled, only the static IPv4 address can be used. (Wenn IPv6 nicht aktiviert ist, kann nur die statische IPv4-Adresse verwendet werden.)

540 Configure a static IPv6 address for your active OA or disable Enclosure IP Mode before enabling DHCP for IPv4. (Konfigurieren Sie eine statische IPv6-Adresse für Ihren aktiven OA oder deaktivieren Sie „Enclosure IP Mode“ (Gehäuse-IP-Modus), bevor Sie DHCP für IPv4 aktivieren.

541 Configure a static IPv4 address for your active OA or disable Enclosure IP Mode before disabling IPv6. (Konfigurieren Sie eine statische IPv4-Adresse für Ihren aktiven OA oder deaktivieren Sie „Enclosure IP Mode“ (Gehäuse-IP-Modus), bevor Sie IPv6 deaktivieren.

542 The submitted URL is invalid for uploading. (Der übermittelte URL ist zum Hochladen ungültig.)

543 This version of Onboard Administrator firmware does not support boot options for servers configured in UEFI Boot mode. (Diese Version der Onboard Administrator-Firmware unterstützt keine Startoptionen für im UEFI-Startmodus konfigurierte Server.)

544 This operation cannot be performed while Secure Boot is enabled. (Dieser Vorgang kann nicht durchgeführt werden, solange der sichere Systemstart aktiviert ist).

545 This operation cannot be performed while Secure Boot is enabled or blade is booting the OS. (Dieser Vorgang kann nicht durchgeführt werden, solange der sichere Systemstart aktiviert ist oder der Blade das Betriebssystem startet.)

561 Transmission from the HP Insight Remote Support receiver was unsuccessful. (Die Übertragung vom HP Insight Remote Support-Empfänger war nicht erfolgreich.)

562 Transmission from the HP Insight Remote Support receiver was unsuccessful. (Die Übertragung vom HP Insight Remote Support-Empfänger war nicht erfolgreich.) Please check connectivity between OA and the Insight Remote Support receiver. (Überprüfen Sie die Konnektivität zwischen OA und dem Insight Remote Support-Empfänger.)

563 The key strength for the provided key is invalid for this configuration. (Die Schlüsselstärke des bereitgestellten Schlüssels ist für diese Konfiguration ungültig.)

564 This command is not supported by the interconnect. (Dieser Befehl wird vom Verbindungsmodul nicht unterstützt.)

565 The string entered is a link-local address and cannot be used for assignment. (Die eingegebene Zeichenfolge ist eine verbindungslokale Adresse und kann nicht zugewiesen werden.)

566 Invalid IPv6 static route gateway. (Ungültiges Gateway für den statischen IPv6-Verbindungsweg.) Es muss ein Verbindungsweg-Gateway angegeben werden und die Angabe darf keine Präfixlänge enthalten.

567 IPv6 static route destination already exists. (Ziel des statischen IPv6-Verbindungswegs ist bereits vorhanden.)

568 Unable to add IPv6 route. (Der IPv6-Verbindungsweg kann nicht hinzugefügt werden.) The maximum number of IPV6 certificates already exist. (Die maximale Anzahl von statischen IPv6-Verbindungswegen ist bereits vorhanden).

569 IPv6 static route not found. (Der statischer IPv6-Verbindungsweg wurde nicht gefunden).

570 Invalid IPv6 static route destination. (Ungültiges Ziel für den statischen IPv6-Verbindungsweg.) Das Ziel des Verbindungswegs muss eine gültige IPv6-Adresse sein.

571 All items cannot be disabled. (Es können nicht alle Elemente deaktiviert werden.)

572 This action requires the OA to be in FIPS Mode ON/DEBUG. (Diese Aktion erfordert, dass sich der OA im FIPS-Modus ON/DEBUG befindet.)

573 Must set MINRATE option if using timeout range. (Bei Verwendung eines Zeitlimitbereichs muss die Option MINRATE eingestellt werden.)

574 Minimum data rate must be larger than 0. (Der Mindestwert für die Datenrate muss größer als 0 sein.)

575 Maximum timeout must be larger than minimum timeout. (Das maximale Zeitlimit muss größer als das minimale Zeitlimit sein.)

576 Timeout must be larger than 0. (Das Zeitlimit muss größer als 0 sein.)

577 HTTP Read Timeout is already set to the requested value. (Für das HTTP-Lesezeitlimit wurde bereits der angeforderte Wert festgelegt.)

Insight Display-Screenshotfehler

1 Missing credentials. (Fehlende Anmeldeinformationen).

2 The getLCDImage CGI process has caught the SIGSEGV signal. (Der getLCDImage-CGI-Vorgang hat das SIGSEGV-Signal empfangen).

3 Could not acquire access to the image in a reasonable amount of time. (Zugriff auf das Image innerhalb eines plausiblen Zeitraums nicht möglich).

4 Cannot open semaphores. (Semaphoren können nicht geöffnet werden).

5 Produce SEMV does not work. („Produce SEMV” funktioniert nicht).

6 Consume SEMV does not work. („Consume SEMV” funktioniert nicht).

7 Cannot lock the image file. (Imagedatei kann nicht gesperrt werden).

8 Cannot open the image file. (Imagedatei kann nicht geöffnet werden).

9 Cannot seek in the image file. (In Imagedatei kann nicht gesucht werden).

10 Unable to resume session. (Sitzung konnte nicht fortgesetzt werden).

11 Insufficient privileges. (Berechtigungen nicht ausreichend).

Werkseinstellungen von Onboard Administrator

Wenn Sie die Werkseinstellungen von HP BladeSystem Onboard Administrator zurücksetzen, wird das Administratorkennwort nicht auf die Werkseinstellung zurückgesetzt. Vielmehr bleibt das zuletzt angegebene Kennwort erhalten. Für den Fall, dass das Administratorkennwort auf die Werkseinstellungen zurückgesetzt werden muss (wie auf dem im Lieferumfang von Onboard Administrator enthaltenen Aufkleber angegeben), lesen Sie den Abschnitt „Wiederherstellen des Administratorkennworts“ (Wiederherstellen des Administratorkennworts auf Seite 15) in diesem Handbuch.

Wenn Onboard Administrator auf die Werkseinstellungen zurückgesetzt wird, werden zudem alle in Onboard Administrator enthaltenen Zertifikate zurückgesetzt.

Onboard Administrator-SNMP-Traps

Der BladeSystem Onboard Administrator unterstützt die folgenden SNMP-Traps.

Trap-ID	Trap-Name	Beschreibung
22001	cpqRackNameChanged	Rack-Name hat sich geändert
22002	cpqRackEnclosureNameChanged	Gehäuse-Name hat sich geändert
22003	cpqRackEnclosureRemoved	Entfernen eines verknüpften Gehäuses erkannt
22004	cpqRackEnclosureInserted	Einfügen eines verknüpften Gehäuses erkannt
22008	cpqRackEnclosureFanFailed	Gehäuselüfter ausgefallen
22009	cpqRackEnclosureFanDegraded	Gehäuselüfter beeinträchtigt
22010	cpqRackEnclosureFanOk	Gehäuselüfter in Ordnung
22011	cpqRackEnclosureFanRemoved	Gehäuselüfter entfernt
22012	cpqRackEnclosureFanInserted	Gehäuselüfter eingesetzt
22013	cpqRackPowerSupplyFailed	Gehäusenetzteil ausgefallen
22014	cpqRackPowerSupplyDegraded	Gehäusenetzteil beeinträchtigt
22015	cpqRackPowerSupplyOk	Gehäusenetzteil in Ordnung
22016	cpqRackPowerSupplyRemoved	Gehäusenetzteil entfernt
22017	cpqRackPowerSupplyInserted	Gehäusenetzteil eingesetzt
22018	cpqRackPowerSubsystemNotRedundant	Gehäuse-Stromversorgungs-Subsystem nicht redundant
22019	cpqRackPowerSubsystemLineVoltageProblem	Leitungsspannungsproblem des Gehäuse-Stromversorgungs-Subsystems
22020	cpqRackPowerSubsystemOverloadCondition	Überlastbedingung des Gehäuse-Stromversorgungs-Subsystems
22028	cpqRackServerBladeRemoved	Blade entfernt (ersetzt durch 22050 in OA v1.30)
22029	cpqRackServerBladeInserted	Blade eingesetzt (ersetzt durch 22051 in OA v1.30)
22037	cpqRackEnclosureManagerDegraded	Onboard Administrator beeinträchtigt
22038	cpqRackEnclosureManagerOk	Onboard Administrator in Ordnung
22039	cpqRackEnclosureManagerRemoved	Onboard Administrator entfernt
22040	cpqRackEnclosureManagerInserted	Onboard Administrator eingesetzt

Trap-ID	Trap-Name	Beschreibung
22041	cpqRackManagerPrimaryRole	Onboard Administrator ist aktiv
22042	cpqRackServerBladeEKeyingFailed	Blade eKeying-Konfiguration fehlgeschlagen
22044	cpqRackNetConnectorRemoved	Verbindungsmodul entfernt
22045	cpqRackNetConnectorInserted	Verbindungsmodul eingesetzt
22046	cpqRackNetConnectorFailed	Verbindungsmodul ausgefallen
22047	cpqRackNetConnectorDegraded	Verbindungsmodul beeinträchtigt
22048	cpqRackNetConnectorOk	Verbindungsmodul in Ordnung
22049	cpqRackServerBladeToLowPower	Blade forderte zu wenig Strom an
22050	cpqRackServerBladeRemoved2	Blade entfernt2
22051	cpqRackServerBladeInserted2	Blade eingesetzt2

Bekannte Browser-Probleme

- **Allgemeine Probleme beim Zugriff auf Anwendungen über Links, die von der Onboard Administrator GUI bereitgestellt werden**

  Damit eine Verwaltungsanwendung ordnungsgemäß funktioniert, wenn über einen Onboard Administrator-Link auf sie zugegriffen wird, muss die Onboard Administrator-Domäne möglicherweise zu Ihren vertrauenswürdigen Sites hinzugefügt werden. Außerdem ist zu beachten, dass die über diese Links geöffneten Verwaltungsanwendungen möglicherweise nicht die gleichen Browserversionen unterstützen, die vom Onboard Administrator unterstützt werden.

- **Verbindungen zu Onboard Administrator schlagen über Internet Explorer und Windows 2003 Active Directory fehl**

  Von OA 4.30 werden einige Verschlüsselungssammlungen aufgrund der allgemein bekannten Schwäche der zugehörigen Verschlüsselungsalgorithmen nicht mehr unterstützt. Damit eine erfolgreiche Verbindung zu Onboard Administrator hergestellt werden kann, müssen Clients eine oder mehrere der in der folgenden Tabelle aufgelisteten Verschlüsselungssammlungen unterstützen. Verbindungsversuche über Internet Explorer und Windows 2003 Active Directory schlagen fehl, da diese Version von Windows für mindestens eine der unterstützten Verschlüsselungssammlungen keine standardmäßig Unterstützung gewährt. Sie können zum Hinzufügen der erforderlichen Unterstützung AES-basierte Verschlüsselungssammlungen in Windows 2003 installieren und aktivieren. Weitere Informationen finden Sie in dem Microsoft Hotfix, der auf der Microsoft Support Website (http://support.microsoft.com/kb/948963) verfügbar ist.

SSL/TLS Cipher Suites	Standardnamen für SSL/TLS-Verschlüsselungssammlungen
EDH-RSA-DES-CBC3-SHA	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

SSL/TLS Cipher Suites	Standardnamen für SSL/TLS-Verschlüsselungssammlungen
DHE-RSA-AES128-SHA	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
DHE-RSA-AES256-SHA	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-DES-CBC3-SHA	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256

- **Probleme mit Mozilla Firefox 3.6 (oder höher)**

  Wenn Sie Mozilla Firefox 3.6 oder höher verwenden, werden durch Drücken der ESC-Taste alle geöffneten XMLHttpRequest-Verbindungen getrennt, was zu einem unerwarteten Verhalten des Clients führen kann. Weitere Informationen finden Sie im Mozilla-Artikel (https://bugzilla.mozilla.org/show_bug.cgi?id=614304).

- **Browser-Probleme unter Betriebssystemen, die vor 2004 veröffentlicht wurden**

  Browser auf Betriebssystemen, die vor 2004 veröffentlicht wurden und auf die nicht die neuesten sicherheitsbezogenen Patches und Aktualisierungen angewandt wurden, können möglicherweise keine Verbindung zur Onboard Administrator-Weboberfläche herstellen. Bei Onboard Administrator 3.70 wurde der Standard-Zertifikat-Hashalgorithmus von SHA1 in SHA256 geändert. SHA256-Unterstützung ist erst nach dem Jahr 2003 allgemein verfügbar. Stellen Sie sicher, dass die folgenden Mindestanforderungen für die SHA256-Unterstützung für die einzelnen Betriebssysteme erfüllt werden:

  - Windows XP erfordert SP3.
  - Windows 2003 Server SP2 erfordert zur Unterstützung von SHA256 eine Aktualisierung. Weitere Informationen finden Sie auf der Microsoft Support-Website (http://support.microsoft.com/kb/968730).
  - RedHat 4 wurde ursprünglich mit OpenSSL 0.9.7 geliefert, das SHA256 nicht unterstützt. Aktualisieren Sie das Betriebssystem mit dem entsprechenden RPM zur Verwendung von OpenSSL 0.9.8 oder höher.

- **Bestimmte Browser können nicht auf Onboard Administrator zugreifen, wenn beim Erstellen des Onboard Administrator-Zertifikats SHA-224 als SSL-Hash-Signatur verwendet wird**

  OA 3.70 ermöglicht die Änderung des Hash-Signatur-Algorithmus. Wenn in Ihrer Netzwerkinfrastruktur ein SHA1-Zertifikat benötigt wird, ändern Sie Schlüsselgröße und Hash-Algorithmus mit dem Onboard Administrator-Befehl `GENERATE KEY`.

HINWEIS: Die Browser Microsoft Internet Explorer, Google Chrome und Safari können möglicherweise nicht auf die Onboard Administrator-Weboberfläche zugreifen, wenn das Onboard Administrator-Zertifikat mit SHA-224 als SSL-Hash-Signatur auf Windows XP, Windows Vista und Windows 7 generiert wird. SHA-224 ist nicht die standardmäßige Hash-Funktion für selbst signierte Onboard Administrator-Zertifikate.

- **Bei einigen Browsern wird die "%scope_id"-Schreibweise bei einer verbindungslokalen IPv6-Adresse nicht unterstützt: bestimmte Onboard Administrator-Funktionen gehen beim Verwenden der Adresse verloren**

  Bei einigen Browsern wird die "%scope_id"-Schreibweise bei einer verbindungslokalen IPv6-Adresse nicht unterstützt. Bestimmte Browser akzeptieren möglicherweise Webadressen mit dieser Schreibweise, aber bestimmte Funktionen gehen beim Zugriff auf den Onboard Administrator über diese Adresse verloren. Zu den betroffenen Onboard Administrator-GUI-Funktionen gehören Insight Display und die Konfigurationssammlung auf dem Bildschirm **Configuration Scripts** (Konfigurationsskripts) (die Funktionen **SHOW CONFIG** und **SHOW ALL**).

- **Google Chrome v27.0.1453.94 funktioniert mit Onboard Administrator 4.01 nicht ordnungsgemäß**

  Chrome lädt keine Abbilder mehr. Andere Inhalte, wie z. B. Skripts, werden erfolgreich geladen. Weitere Einzelheiten finden Sie in den Google-Problem-Bericht (http://code.google.com/p/chromium/issues/detail?id=244043).

Bekannte Netzwerkprobleme

- **Bei der Emulex-Firmware vor Version 4.1.450.7 ist DCC bei einer physischen 10 GB-Verbindung nicht verfügbar**

  Aufgrund eines Problems mit der Emulex-Firmware vor Version 4.1.450.7 ist die DCC bei einer physischen 10 GB-Verbindung möglicherweise nicht verfügbar. Wenn dieses Problem bei G7 und Gen8 Server Blades voller Bauhöhe (einschließlich HP ProLiant BL680 G7, BL685c G7, BL620 G7 und BL660 Gen8) mit in einer Virtual Connect-Umgebung konfigurierten HP NC55x LOMs oder FLB554 FlexibleLOMs vorliegt, kann bei einer Aktualisierung der OA-Firmware von Version 3.56 oder früher auf Version 3.60 oder höher die Netzwerkverbindung verloren gehen.

  Um einen Verlust der Netzwerkverbindung während der Firmwareaktualisierung von Onboard Administrator zu verhindern, stellen Sie vor der Aktualisierung sicher, dass die Firmware des Netzwerkadapters aktualisiert wurde, um den nicht verfügbaren Zustand der DCC zu beheben, wie in der Kundenmitteilung c03600027 empfohlen (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03600027). Weitere Informationen finden Sie in diesem Kundenratschlag.

Verschiedene bekannte Probleme

- **Abgelehnter CLI-Zugriff mittels eines SSH-Schlüssels**

  Bei dem Versuch, sich mittels eines SSH-Schlüssels bei der Onboard Administrator-CLI anzumelden, wird der Zugriff möglicherweise abgelehnt. In diesem Fall werden Sie zur Eingabe eines Kennwortes aufgefordert. Dieses Problem kann auftreten, wenn der FIPS-Modus aktiviert ist, nachdem der Onboard Administrator von Version 3.7x auf eine höhere Version aktiviert wurde. Einige Dritthersteller-Utility-Tools erstellen Schlüssel, die kleiner als die in der aktuellen Version von Onboard Administrator zulässige Mindestlänge sind. Stellen Sie sicher, dass die Länge des installierten Schlüssels mindestens 2048 Bits beträgt. Weitere Informationen zu den Anforderungen bezüglich der SSH-Schlüsselgröße (insbesondere der Größe des SSH-Standardschlüsseltyps) finden Sie in der Tabelle unter „Kryptographische Sicherheitsfunktionen

und Standardeinstellungen“ (Kryptographische Sicherheitsfunktionen und Standardeinstellungen auf Seite 18).

- **Verbindung zum Onboard Administrator kann nach einem Neustart nicht wieder hergestellt werden („Trusted Hosts“ (Vertrauenswürdige Hosts) aktiviert)**

  Wenn „Trusted Hosts“ (Vertrauenswürdige Hosts) aktiviert ist, schlägt der Versuch, die Verbindung zum Onboard Administrator über einen Client wieder herzustellen, der auf einem Betriebssystem mit RFC 4941-Unterstützung gehostet wird, möglicherweise fehl, nachdem das Betriebssystem neu gestartet wurde.

  RFC 4941 beschreibt eine Erweiterung des IPv6-SLAAC, die das Erstellen globaler temporärer IPv6-Adressen unter Verwendung von Schnittstellenkennungen ermöglicht, die sich im Laufe der Zeit ändern. Wenn ein Betriebssystem mit RFC 4941-Unterstützung (wie z. B. Windows 7) neu gestartet wird oder wenn die aktuelle Adresse abläuft, wird eine neue temporäre IPv6-Adresse erstellt. Beim Zugriff auf Onboard Administrator über einen Client, der auf einem Betriebssystem mit RFC 4941-Unterstützung gehostet wird, wird die Verbindung nach einem Neustart aufgrund der neuen IPv6-Adresse des Clients und der daraus resultierenden Unstimmigkeit zwischen dieser Adresse und der für den Client in der Liste „Trusted Addresses“ (Vertrauenswürdige Adressen) konfigurierten IPv6-Adresse nicht mehr hergestellt.

  Um dieses Problem zu vermeiden, deaktivieren Sie entweder das Erstellen globaler temporärer IPv6-Adressen im Betriebssystem oder konfigurieren Sie die IP-Adresse des vertrauenswürdigen Hosts mit der IPv6-Adresse des neu erstellten Clients neu.

- **Zertifikaterstellung schlägt fehl (Fehlermeldung `Could not generate the CSR`)**

  Bei dem Versuch, ein Zertifikat über den aktiven oder den Standby-Onboard Administrator oder mit dem CLI-Befehl GENERATE CERTIFICATE zu erstellen, wird die Fehlermeldung `Could not generate the CSR` (CSR konnte nicht erstellt werden) ausgegeben. Dies tritt bei dem Versuch auf, entweder ein selbstsigniertes Zertifikat oder eine Zertifikatssignierungsanforderung (CSR) zu erstellen, wobei obligatorische und optionale Informationen bereitgestellt werden.

  Dieses Problem wird möglicherweise dadurch verursacht, dass der optionale alternative Name inkorrekt angegeben wurde. Der alternative Name muss 0-511 Zeichen lang sein, und wenn sein Wert nicht 0 ist, muss er eine Liste von Schlüsselwort:Wert-Paaren enthalten, die durch Kommas getrennt sind. Zu den gültigen Schlüsselwort:Wert-Einträgen gehören IP:<IP-Adresse> und DNS:<Domänenname>.

- **Versuchtes Hinzufügen (Hochladen) eines ZS-Benutzerzertifikats schlägt mit einer Überprüfungsfehlermeldung fehl**

  Bei dem Versuch, ein Zertifikat zur Registerkarte **Local Users (Lokale Benutzer)> Administrator > Certificate Information (Zertifikatinformationen)** hinzuzufügen, wird folgende Fehlermeldung angezeigt:

  ```
  The user certificate could not be verified. (Das Benutzerzertifikat
  konnte nicht überprüft werden). Bitte laden Sie das entsprechende ZS-
  Zertifikats hoch.
  ```

  Grund und Lösung: Das ZS-Zertifikat der Zertifizierungsstelle, von der dieses Benutzerzertifikat ausgestellt wurde, muss über die Registerkarte „Two-Factor Authentication Certificate Upload“ (Zertifikat-Upload für 2-Faktor-Authentifizierung) installiert werden.

- **Begrenzen Sie die Anzahl der gleichzeitigen iLO Virtual Media-Sitzungen, um Zeitüberschreitungs- und Leistungsprobleme zu vermeiden**

  Die Leistung von HP c-Class BladeSystem ProLiant und Integrity iLO Virtual Media wird durch die Aktivität und Anzahl gleichzeitiger iLO Virtual Media-Sitzungen und die OA-Auslastung eingeschränkt. Die Onboard Administrator-Gehäuse-DVD- und Enclosure Firmware

Management-Funktionen nutzen die iLO Virtual Media-Funktion und weisen möglicherweise ähnliche Leistungseinschränkungen auf.

Um Zeitüberschreitungsprobleme der Medien zu vermeiden, empfiehlt HP, die Anzahl gleichzeitiger Sitzungen einzuschränken. Sollten während der Betriebssysteminstallation oder während Firmwareaktualisierungen Zeitüberschreitungsprobleme auftreten, dann verringern Sie die Anzahl laufender virtueller Medien-Sitzungen und starten Sie den Vorgang neu.

- **Der Onboard Administrator-Link zur iLO 3 Integrated Remote Console startet manchmal möglicherweise nicht**

  Der OA-Link zur iLO 3 Integrated Remote Console startet manchmal möglicherweise nicht. Weitere Informationen zum Beheben dieses Problems finden Sie im Kundenratschlag c03077476 (http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03077476).

- **Denial-of-Service beim Herstellen einer Verbindung zum OA-Webserver**

  Versuche, eine Verbindung zum OA-Webserver herzustellen, werden aufgrund eines Denial-of-Service-Angriffs (wie z. B. eines Slowloris-Angriffs) verweigert. Bei einem solchen Angriff öffnet ein schädlicher Client viele TCP-Verbindungen, um alle verfügbaren Verbindungen zu belegen. Mit dem Onboard Administrator-CLI-Befehl `SET HTTP REQUESTREADTIMEOUT` können die Auswirkungen von Angriffen durch schädliche Webserver-Clients verringert werden. Weitere Informationen finden Sie im *HP BladeSystem Onboard Administrator Befehlszeilenschnittstelle Benutzerhandbuch*.

- **EFM-Ermittlungs-/Aktualisierungsvorgänge schlagen fehl – nicht unterstützte Größe des ISO-Image**

  OA unterstützt nur SPP-ISO-Images kleiner als 4 GB. Bei einem Image von 4 GB oder größer schlägt die EFM-Funktionalität fehl. Der OA CLI-Befehl `SHOW FIRMWARE MANAGEMENT` zeigt als ISO-URL-Status `Invalid URL` an.

  Sie müssen ein benutzerdefiniertes ISO-Image erstellen, aus dem die Komponenten ausgeschlossen werden, die für die OA-EFM-Blade-Firmwareaktualisierung nicht benötigt werden. Weitere Informationen finden Sie unter „Enclosure Firmware Management“ (siehe Enclosure Firmware Management auf Seite 197).

- **Seite „Users/Authentication (LDAP)“ (Benutzer/Authentifizierung (LDAP)) (Directory Settings** (Verzeichniseinstellungen) **wird nach einem Upgrade von bestimmten älteren Versionen von OA nicht geladen**

  Nachdem OA im FIPS-Modus ON/DEBUG von älteren Versionen (Versionen 3.71 bis 4.11) auf 4.20 oder höher aktualisiert wurde, wird die Seite **Users/Authentication (Benutzer/Authentifizierung) >Directory Settings (Verzeichniseinstellungen)** nicht mehr geladen. Die folgende Meldung wird angezeigt:

  ```
  Die Schlüsselstärke des bereitgestellten Schlüssels ist für diese Konfiguration ungültig.
  ```

  Dies lässt sich auf die stärkeren Sicherheitsfunktionen zurückführen, die ab OA 4.20 implementiert wurden. Die Mindestlänge von Schlüsseln wurde auf 2048 Bits erhöht. Die Fehlermeldung bedeutet, dass OA LDAP-Zertifikate mit nicht konformen Schlüsseln ermittelt hat, die auf der älteren Version von OA installiert worden sind.

  Der OA-Administrator muss die nicht konformen Schlüssel entfernen und sie durch Schlüssel ersetzen, die 2048 Bits oder größer sind.

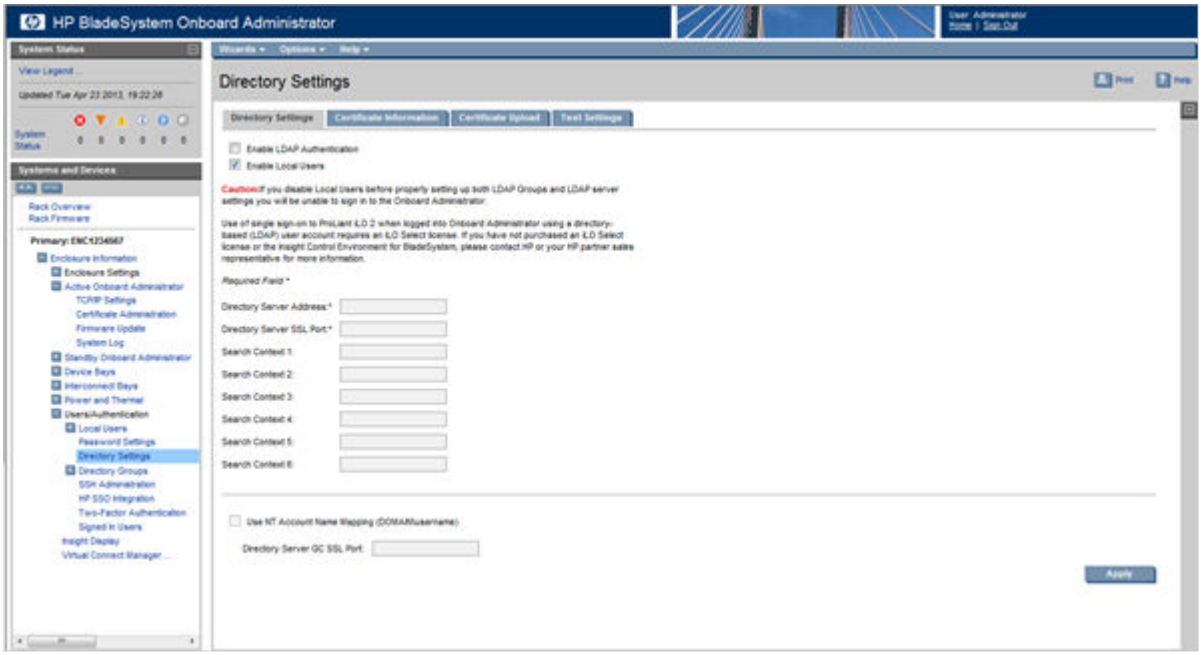
12 Aktivieren der LDAP-Directory Services-Authentifizierung bei Microsoft Active Directory

Zertifizierungsdienste

Die Microsoft® Implementierung von LDAP über SSL erfordert, dass die Domänencontroller DC-Zertifikate von der Zertifizierungsstelle (CA) der Organisation installieren. Dieser Vorgang findet statt, wenn der Dienst einer Zertifizierungsstelle des Organisationsstammes in Active Directory zu einem Server hinzugefügt wird. HP rät sehr dazu, eine Zertifizierungsstelle des Organisationsstammes zu verwenden, da das Anfordern und Akzeptieren von DC-Zertifikaten sich dadurch weniger komplex als bei einer Standalone-Zertifizierungsstelle gestaltet.

HINWEIS: Die LDAP-Funktion von Onboard Administrator unterstützt Microsoft® Active Directory mittels des Attributs `memberOf`. Mittels des Attributs `groupMembership` wird auch Novell eDirectory unterstützt. OpenLDAP wird nicht unterstützt.

Vorbereiten des Verzeichnisses



So bereiten Sie das Verzeichnis vor:

1. Erstellen Sie eine Active Directory-Gruppe namens „OA Admins“ (OA-Administratoren), und fügen Sie dieser Gruppe einen Benutzer namens „TestAdmin“ hinzu.
2. Erstellen Sie eine Gruppe namens „OA Operators“ (OA-Bediener), und fügen Sie dieser Gruppe dann einen Benutzer namens „TestOperator“ hinzu. Die Benutzerberechtigungen sind bedeutungslos.

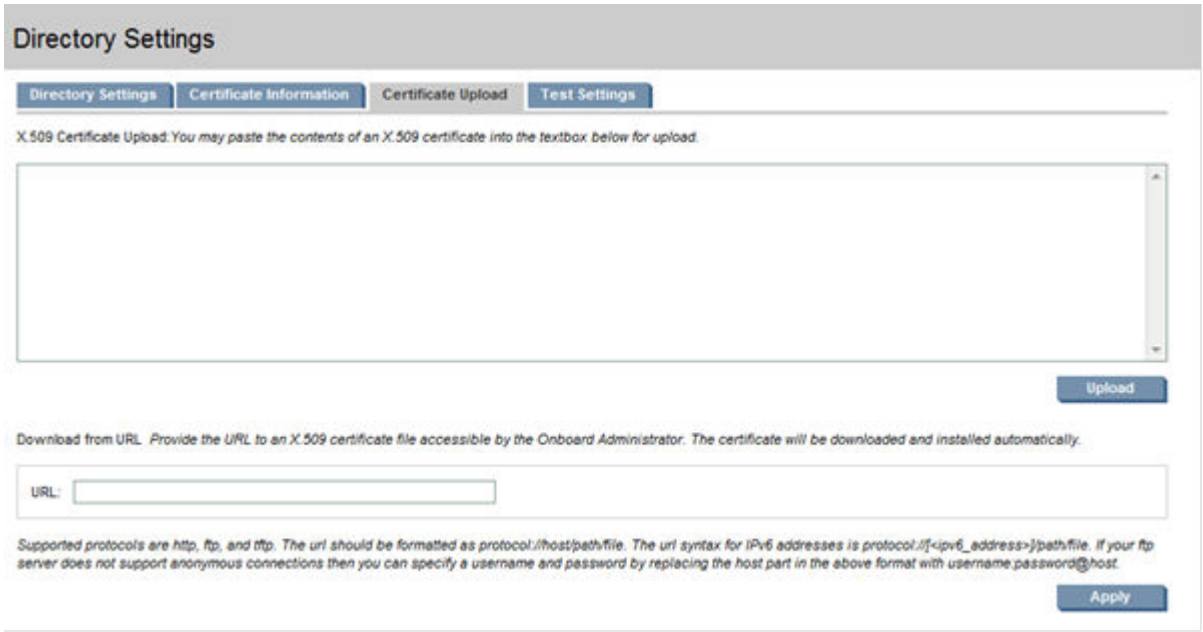
3. Navigieren Sie zum Bildschirm „Directory Settings“ (Verzeichniseinstellungen) unter „Users/ Authentications“ (Benutzer/Authentifizierungen) für das Gehäuse.
4. Klicken Sie auf **Enable LDAP** (LDAP aktivieren), und geben Sie die IP-Adresse oder den Namen eines Ihrer Domänencontroller ein. Weitere Informationen zum Überprüfen, ob der DC Port 636 abhört, finden Sie unter „Fehlerbehebung von LDAP auf dem Onboard Administrator“ (Fehlerbeseitigung für LDAP auf Onboard Administrator auf Seite 396). Alternativ dazu können Sie anstatt eines Servernamens den Domänennamen Ihrer AD-Domäne (DOMAIN.COM) eingeben. Dadurch werden die für die Domäne definierten DNS-Server zur Bereitstellung von DCs gezwungen. HP empfiehlt, während der Erstkonfiguration zur Vereinfachung eine einzelne IP-Adresse zu verwenden. „Search Context“ (Suchkontext) ist das LDAP-Standardformat. Angenommen, Ihre Benutzerkonten befinden sich in der OU „Users“ in einer Domäne namens „BLADEDEMO.HP.COM“, dann lautet der Suchkontext folgendermaßen:

   CN=Users,DC=bladedemo,DC=hp,DC=com

Hochladen des DC-Zertifikats (optional)

Sie können mehrere DC-Zertifikate hochladen. Laden Sie ein Zertifikat hoch, das LDAP über SSL gestattet.

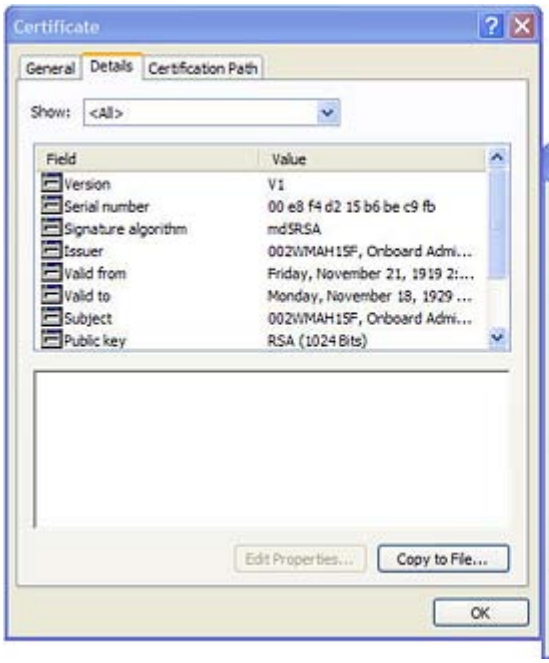
1. Klicken Sie auf die Registerkarte **Upload Certificate Tab** (Zertifikat-Upload).


Directory Settings
Directory Settings
Certificate Information
Certificate Upload
Test Settings
X.509 Certificate Upload You may paste the contents of an X.509 certificate into the textbox below for upload.
Upload
Download from URL Provide the URL to an X.509 certificate file accessible by the Onboard Administrator. The certificate will be downloaded and installed automatically.
URL:
Supported protocols are http, ftp, and tftp. The url should be formatted as protocol://host/path/file. The url syntax for IPv6 addresses is protocol://[<ipv6_address>]/path/file. If your ftp server does not support anonymous connections then you can specify a username and password by replacing the host part in the above format with username:password@host.
Apply

2. Beziehen Sie das Zertifikat vom Domänencontroller, indem Sie in einem Browser-Fenster zu https://*domain_controller*> 636 navigieren (wobei *domain_controller* Ihr Domänencontroller ist). Da dies ein sicherer HTTPS URL ist, werden Sie zum Akzeptieren eines Zertifikats aufgefordert. Wählen Sie **Zertifikat anzeigen**.

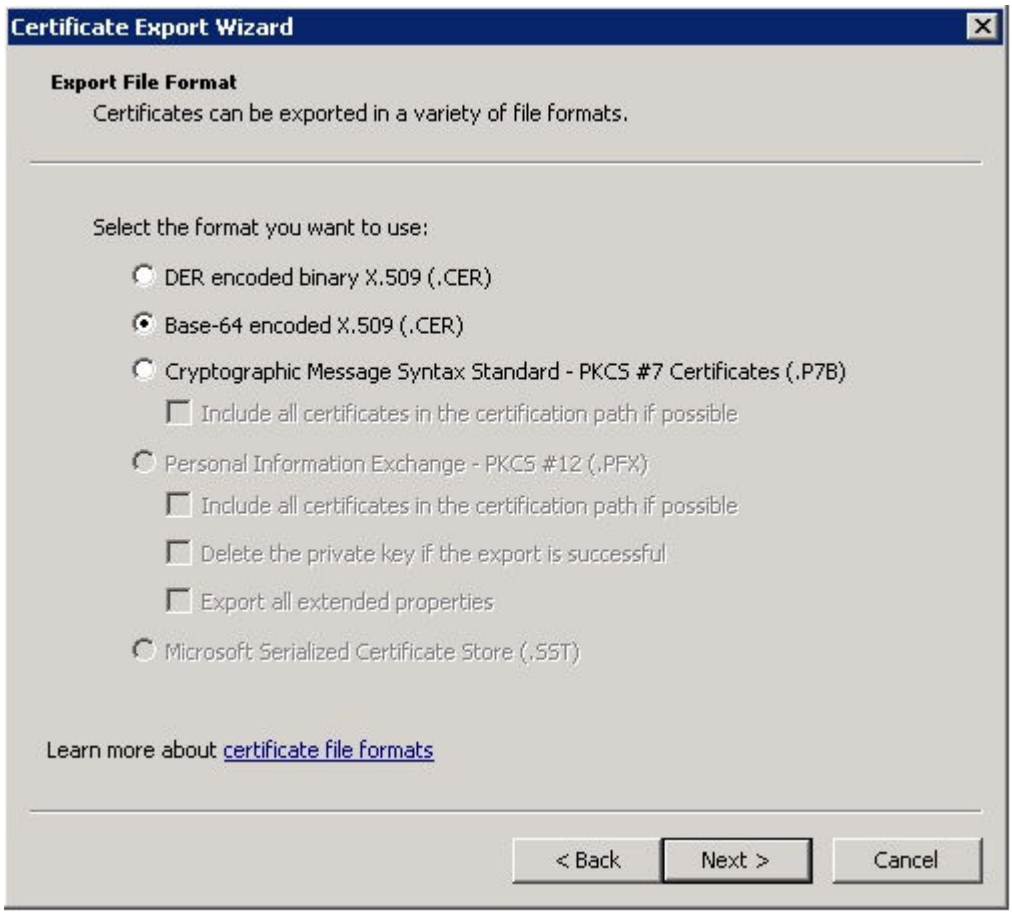
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate has expired or is not yet valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

3. Klicken Sie auf die Registerkarte **Details** und anschließend auf **Copy to File** (In Datei kopieren).



Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

4. Wählen Sie aus der Liste der Exportoptionen **Base-64-codiert x.509 (.CER)** aus (dies ist wichtig). Geben Sie einen Namen und einen Speicherort für die Datei (c:\dccert.cer) an, und beenden Sie den Assistenten.


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

5. Machen Sie die exportierte Zertifikatdatei im Explorer ausfindig, und benennen Sie sie mit der Erweiterung „.txt“ um (z. B. „dccert.txt“). Öffnen Sie die Datei im Editor, und kopieren Sie den gesamten Inhalt in die Zwischenablage. Es folgt ein Beispiel für den Inhalt der Zertifikatdatei:

```
-----BEGIN CERTIFICATE-----
MIIFxDCCBKygAwIBAgIKJWUSwAAAAAAAAjANBgkqhkiG9w0BAQUFADBVMRMwEQYK
CZImiZPyLGQBGRYDY29tMRIwEAYKCZImiZPyLGQBGRYCaHAxFzAVBgoJkiaJk/Is
ZAEZFgdhdGxkZW1vMREwDwYDVQQDEwh3aW5kb3pDQTAeFw0wNjA4MjIyMDIzMTFa
Fw0wNzA4MjIyMDIzMTFaMCAxHjAcBgNVBAMTFXdpbmRvei5hdGxkZW1vLmhwLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAy4zeh3iXydUAWKVHIDsxLJ6B
aRuVT9ZhkL5NQHIDeRjumsgc/jHSERDmHuyoY/qbF7JMhJ9Lh9QQHUg8QfEYsC1y
qTvgisrZeHtvmrmecvSxZm27b4Bj5XYN0VYcrwqKnH7X/tVhmwqGls7/YZyahNU1
lGB2OjoCq5eJxX+Ybx0CAwEAAaOCA00wggNJMAsGA1UdDwQEAwIFoDBEBgkqhkiG
9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4D
…Ausgabe abgeschnitten…
```

```
-----END CERTIFICATE-----
```

6. Kehren Sie zum Bildschirm „Certificate Upload“ (Zertifikat-Upload) von Onboard Administrator zurück, fügen Sie den Inhalt des Zertifikats in das Fenster ein, und klicken Sie dann auf **Upload** (Hochladen).

Erstellen von Verzeichnisgruppen

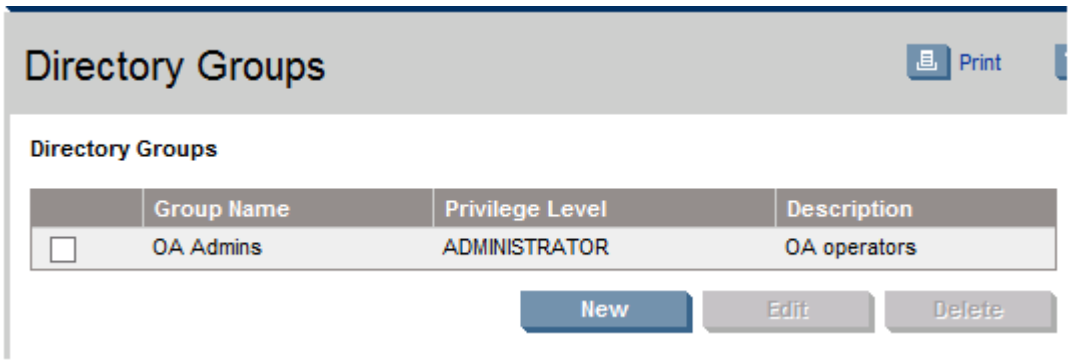
Wenn Onboard Administrator Benutzer authentifiziert und ihnen Berechtigungen zuweist, wird zuerst überprüft, ob der Benutzername und das Kennwort, die in Onboard Administrator eingegeben wurden, mit den Anmeldeinformationen im Verzeichnis übereinstimmen. Wenn eine Entsprechung gefunden wird, fragt Onboard Administrator das Verzeichnis ab, um die Namen der Active Directory-Gruppen herauszufinden, denen der Benutzer angehört. Onboard Administrator vergleicht diese Gruppennamen dann mit den in Onboard Administrator vorhandenen Verzeichnisgruppennamen. Im folgenden Beispiel werden in diesem Schritt Onboard Administrator Verzeichnisgruppen erstellt. Der Gruppenname wird zur Ermittlung der Gruppenmitgliedschaft von LDAP-Benutzern verwendet und muss einer der folgenden fünf Eigenschaften einer Verzeichnisgruppe entsprechen: „Name“ (Name), „Distinguished Name“ (Eindeutiger Name), „Common Name“ (Allgemeiner Name), „Display Name“ (Anzeigename) oder „SAM Account Name“ (SAM-Konto-Name).

So erstellen Sie eine Verzeichnisgruppe:

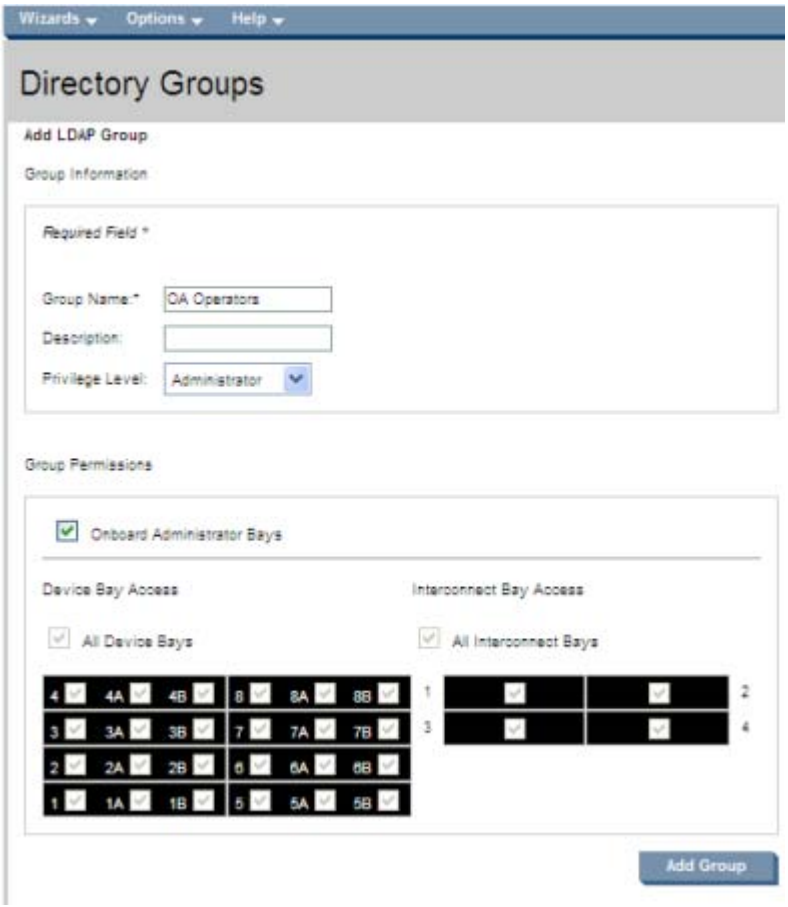
1. Navigieren Sie in Onboard Administrator zum Link **Users>Authentications>Directory Groups** (Benutzer>Authentifizierungen>Verzeichnisgruppen).
2. Um eine neue Verzeichnisgruppe hinzuzufügen, klicken Sie auf **New** (Neu).
3. Erstellen Sie eine Gruppe namens „OA Admins“ (OA-Administratoren), wobei es sich um den gleichen, in Active Directory erstellten Namen handelt.

HINWEIS: Gruppennamen mit Leerstellen werden auf einigen LDAP-Servern möglicherweise nicht unterstützt.

4. Weisen Sie dieser Gruppe uneingeschränkte Verwaltungsberechtigungen über alle Servereinschübe und Verbindungsmoduleinschübe zu, und klicken Sie dann auf **Add Group** (Gruppe hinzufügen).



5. Erstellen Sie unter „Second Directory Group“ (Zweite Verzeichnisgruppe) eine Gruppe namens „OA Operators“ (OA-Bediener), entsprechend der in Active Directory erstellten Bedienergruppe. Weisen Sie der Gruppe anstelle der Berechtigung „Administrator“ die Bedienerberechtigungsstufe zu, und gestatten Sie der Gruppe keinen Zugriff auf Servereinschübe, sondern nur Zugriff auf Verbindungsmoduleinschübe, und klicken Sie auf **Add** (Hinzufügen).



Wenn die Onboard Administrator-Firmware von 2.40 auf 2.31 herabgestuft wird, gehen bis auf die ersten fünf Gruppen alle weiteren Gruppen verloren. Version 2.40 von Onboard Administrator unterstützt 20 Gruppen, während ältere Versionen nur fünf Gruppen unterstützen.

Testen der Verzeichnisanmeldelösung

1. Melden Sie sich bei der aktuellen Onboard Administrator-Sitzung an, und schließen Sie dann alle Browser-Fenster.
2. Navigieren Sie zu Onboard Administrator, und melden Sie sich mit einer der folgenden Optionen an:
   - TestAdmin
   - TestAdmin@Domäne.com
   - DOMÄNE\TestAdmin
   - FQDN: cn=<TestAdmin>,cn=<Benutzer>dc=<Domäne>,dc=<com>

3. Geben Sie das entsprechende Kennwort für das Benutzerkonto ein. Wenn Sie sich nicht mit uneingeschränkten Administratorberechtigungen anmelden können, schlagen Sie unter „Fehlerbehebung von LDAP auf dem Onboard Administrator“ (Fehlerbeseitigung für LDAP auf Onboard Administrator auf Seite 396) nach. Beachten Sie bitte, dass Sie sich nicht mit Ihrem Benutzernamen anmelden können. Lautet der Kontoname beispielsweise „Jonas Meiser“ und das Konto „jmeiser“, ist keine Anmeldung unter „jmeiser“ möglich, da dieses Format derzeit nicht von LDAP unterstützt wird.
4. Melden Sie sich von Onboard Administrator ab, und melden Sie sich dann mit einer der folgenden Optionen an:
   - TestOperator
   - TestOperator@Domäne.com
   - DOMÄNE\TestOperator
   - FQDN: cn=<TestOperator>,cn=<Benutzer>dc=<Domäne>,dc=<com>
5. Geben Sie das entsprechende Kennwort für dieses Konto ein. Sie haben uneingeschränkten Zugriff auf die Verbindungsmoduleinschübe, jedoch nicht auf irgendwelche Server Blades.

Fehlerbeseitigung für LDAP auf Onboard Administrator

Um zu überprüfen, ob SSL auf den Domänencontrollern in Ihrer Domäne funktioniert, öffnen Sie einen Browser, und navigieren Sie dann zu https://*<domain_controller>*:636 (geben Sie anstelle von domain_controller Ihren Domänencontroller ein). Sie können anstelle von <Domänencontroller> <Domäne> eingeben, um beim DNS anzufragen, welcher Domänencontroller zurzeit Anforderungen für die Domäne beantwortet. Testen Sie mehrere Domänencontroller, um sicherzustellen, dass allen ein Zertifikat ausgestellt wurde. Wenn SSL auf einem Domänencontroller ordnungsgemäß funktioniert (ihm wurde z. B. ein Zertifikat ausgestellt), werden Sie im Dialogfeld „Security“ (Sicherheit) gefragt, ob Sie mit dem Zugriff auf die Site fortfahren oder das Zertifikat einsehen möchten. Wenn Sie auf „Yes“ (Ja) klicken, wird keine Webseite angezeigt. Der Test besteht darin, das Sicherheitsdialogfeld aufzurufen. Ein Server, der keine Verbindungen an Port 636 akzeptiert, zeigt die Meldung `page cannot be displayed` (Seite kann nicht angezeigt werden) an. Schlägt dieser Test fehl, akzeptiert der Domänencontroller keine SSL-Verbindungen, da ihm möglicherweise kein Zertifikat ausgestellt wurde. Dieser Vorgang läuft automatisch ab, macht möglicherweise jedoch einen Neustart erforderlich.

So vermeiden Sie einen Neustart:

1. Laden Sie auf dem Domänencontroller das MMC-Snap-In „Computer Account“ (Computerkonto), und navigieren Sie dann zum Ordner „Personal->Certificates“ (Persönlich->Zertifikate).
2. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Request New Certificate** (Neues Zertifikat anfordern). Der Standardtyp ist „Domain Controller“ (Domänencontroller).
3. Klicken Sie auf **Next** (Weiter), und wiederholen Sie den Vorgang, bis der Domänencontroller das Zertifikat ausstellt.

Als zweite Methode der Fehlerbehebung für SSL kann auf dem Domänencontroller folgender Befehl ausgegeben werden:

```
C:\netstat -an | find /i "636"
```

Wenn der Server Port 636 auf Anforderungen abhört, sollte folgende Antwort erscheinen:

```
 TCP   0.0.0.0:636      0.0.0.0:0        LISTENING
```

1. Als drittes Problem ist es möglich, dass die Domänencontroller nicht automatisch eingetragen wurden. Es kann bis zu acht Stunden dauern, bis die Domänencontroller automatisch eingetragen werden und ihre Zertifikate erhalten, da Microsoft die Domänencontroller mit GPO auf ihre neu installierten Zertifizierungsstellen aufmerksam macht. Sie können dies erzwingen, indem Sie auf den Domänencontrollern DSSTORE -pulse ausführen (das Tool befindet sich in w2k reskit). Dies wird durch winlogon ausgelöst. Damit die automatische Eintragung funktioniert, müssen Sie sich daher möglicherweise ab- und wieder anmelden. Die Zertifikate erscheinen automatisch in der Liste „CAs Issued Certs“ (Von Zertifizierungsstellen ausgegebene Zertifikate). Vergewissern Sie sich, dass die Zertifizierungsstelle sie nicht unter „Pending Certs“ (Anstehende Zertifikate) aufführt. Wenn dies der Fall ist, ändern Sie die Zertifizierungsstelle, sodass Zertifikate automatisch ausgegeben werden, wenn eine Anforderung eingeht. Wenn die Funktion für die automatische Registrierung weiterhin nicht funktioniert, fordern Sie das Zertifikat mittels des folgenden Verfahrens an.
2. Öffnen Sie auf dem Domänencontroller MMC, und fügen Sie das Zertifikat-Snap-In („Computer Account“ (Computerkonto)) hinzu.
3. Navigieren Sie zu Personal (Persönlich), und klicken Sie dann mit der rechten Maustaste auf den Ordner.
4. Klicken Sie auf **Request New Cert** (Neues Zertifikat anfordern) und dann auf **Next** (Weiter).
5. Geben Sie einen Namen für das Zertifikat ein.

Sollte ein RPC-Fehler auftreten, überprüfen Sie, ob die Zertifizierungsstelle in DNS aufgelistet wird und ob die Zertifizierungsstelle ausgeführt wird.

Wird der Assistent nicht gestartet, bewirken Sie, dass der Server die Zertifizierungsstelle sieht, und gestatten Sie dem Assistenten dann die Ausführung:

Um den GPO-Vorgang zu beschleunigen und die Domänencontroller zur Bestätigung der Zertifizierungsstelle zu veranlassen, verwenden Sie einen der folgenden Befehle:

- Windows® 2003, Gpupdate /force
- Windows® 2000, Secedit /refreshpolicy machine_policy /enforce

Vergewissern Sie sich, dass Onboard Administrator über alle entsprechenden Netzwerkeinstellungen, die für Ihr Netzwerk eindeutig sind, (wie z. B. DNS) verfügt und dass Uhrzeit und Datum richtig sind (für Zertifikate ist das Datum bedeutsam). Stellen Sie sicher, dass Onboard Administrator den DNS-Server erreichen kann (senden Sie von der Befehlszeilenschnittstelle des Onboard Administrator-Moduls einen Ping-Befehl an den Server).

Wenn LDAP beim Starten im Modus „Lost Password“ (Verlorenes Kennwort) aktiviert ist, wird das lokale Administratorkennwort zurückgesetzt, wird LDAP deaktiviert und wird die lokale Anmeldung wieder aktiviert.

HINWEIS: Die LDAP-Funktion von Onboard Administrator unterstützt Microsoft® Active Directory mittels des Attributs `memberOf`. Mittels des Attributs `groupMembership` wird auch Novell eDirectory unterstützt. OpenLDAP wird nicht unterstützt.

13 Erstellen von Zertifizierungsstellen und Konfigurieren der 2-Faktor-Authentifizierung für lokale Benutzer- und LDAP-Gruppenkonten

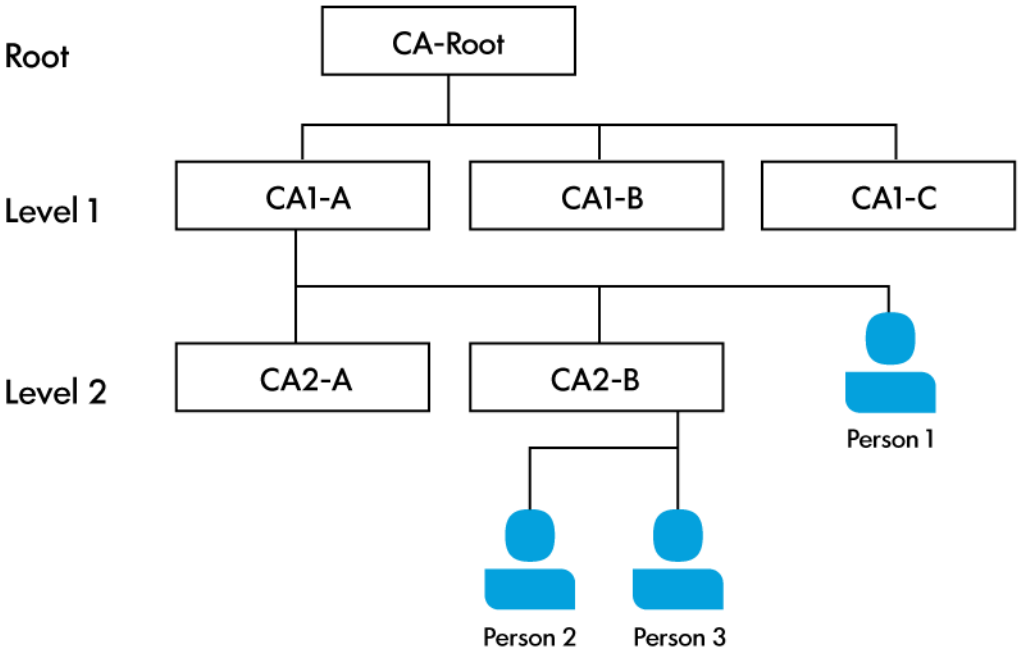
Einführung

Die 2-Faktor-Authentifizierung ist eine optionale Funktion, die verbesserte Sicherheit für den Onboard Administrator bietet. Um Zugriff auf Onboard Administrator zu gewähren, fordert die 2-Faktor-Authentifizierung etwas im Besitz des Benutzers (ein Zertifikat) und etwas dem Benutzer bekanntes (ein Kennwort oder eine PIN) an. Das Zertifikat wird direkt in einem Browser oder auf dem Zugriffsgerät (als Smart Card, Dongle oder TPM) gespeichert.

Sie können die 2-Faktor-Authentifizierung mit lokalen Benutzerkonten oder Verzeichnis- (LDAP-) Gruppenkonten verwenden. Für LDAP-Konten kann zur Angabe des LDAP-Anmeldenamens der Antragsteller oder der alternative Antragstellername verwendet werden. In allen Fällen muss das Benutzerzertifikat anhand einer Zertifizierungsstelle (ZS) überprüft werden.

Infrastrukturzuordnung öffentlicher Schlüssel der 2-Faktor-Authentifizierung

Die Rangordnung der Zertifizierungsstellen basiert auf einer Baumstruktur. Stammzertifikate sind selbstsigniert. Alle anderen Zertifikate können über das Feld des Zertifikatausstellers zum Stammzertifikat zurückverfolgt werden. Benutzerzertifikate können von jeder beliebigen Zertifizierungsstelle in der Struktur ausgegeben werden. Da Onboard Administrator über eingeschränkten Speicherplatz verfügt, wird das Speichern von maximal 12 ZS-Zertifikaten unterstützt. Das folgende Diagramm zeigt eine Baumstruktur ähnlich der, die in den folgenden Beispielen verwendet wird.



ZS-Zuordnungen können sehr einfach oder komplex sein. Ein Beispiel für eine komplexe Zuordnung ist die Infrastruktur öffentlicher Schlüssel des US-Verteidigungsministeriums (http://iase.disa.mil/pki-pke/interoperability/).

Schritte zum Erstellen von Zertifizierungsstellen und zum Konfigurieren der 2-Faktor-Authentifizierung mit lokalen Benutzer- und LDAP-Gruppenkonten

Die folgenden Abschnitte enthalten Anweisungen und Beispiele zum Erstellen von Zertifizierungsstellen und zum Konfigurieren der 2-Faktor-Authentifizierung mit lokalen Benutzer- und LDAP-Gruppenkonten. Zur Vereinfachung werden die ZS-Zertifikate in den angeführten Beispielen auf einem einzelnen System anstelle auf mehreren Systemen erstellt. An einer echten ZS-Implementierung wären mehrere Systeme beteiligt.

Die folgende Tabelle führt die Schritte zum Einrichten der 2-Faktor-Authentifizierung mit lokalen Benutzer- und LDAP-Gruppenkonten auf und gibt den jeweiligen Abschnitt an, in dem die einzelnen Schritte sowie alle untergeordneten Schritte dokumentiert werden.

Schritt	Abschnitt
1	Konfigurieren der Verzeichnisse (Konfigurieren der Verzeichnisse auf Seite 400) • Erstellen der anfänglichen Verzeichnisse für die Stammzertifizierungsstelle • Ändern und Speichern einer OpenSSL-Konfigurationsdatei in jeder Zertifizierungsstelle • Abändern der Standardverzeichnisse passend für Ihre Struktur
2	Erstellen einer Stammzertifizierungsstelle (Erstellen einer Stammzertifizierungsstelle auf Seite 402) • Kopieren der OpenSSL-Konfigurationsdatei zur Stammzertifizierungsstelle • Erstellen des Stamm-ZS-Zertifikats und privaten Schlüssels • Erstellen einer kombinierten PEM-Datei aus einem öffentlichen Stamm-ZS-Schlüssel und einem Zertifikat
3	Erstellen untergeordneter Zertifizierungsstellen (Erstellen untergeordneter Zertifizierungsstellen auf Seite 404) • Erstellen der Verzeichnisse für die untergeordneten Zertifizierungsstellen

Schritt	Abschnitt
	• Bereitstellen von x509-Zertifikatinformationen • Erstellen einer Zertifikatsignieranforderung und eines Serverschlüssels für jede untergeordnete Zertifizierungsstelle • Signieren der Zertifikatsignieranforderung durch die Stammzertifizierungsstelle
4	Erstellen von Benutzerschlüsseln und Zertifikatsignieranforderungen (Erstellen von Benutzerschlüsseln und Zertifikatsignieranforderungen auf Seite 406) • Erstellen der Verzeichnisse für die Benutzerschlüssel und Zertifikatsignieranforderungen • Bereitstellen von x509-Zertifikatinformationen • Erstellen einer Zertifikatsignieranforderung und eines Serverschlüssels für jeden Benutzer • Signieren der Zertifikatsignieranforderung durch die entsprechende untergeordnete Zertifizierungsstelle
5	Überprüfen von Zertifikaten (Überprüfen von Zertifikaten auf Seite 410)
6	Speichern eines Benutzerzertifikats auf einer Smart Card oder einem Browser
7	Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung anhand lokaler Konten (Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung anhand lokaler Konten auf Seite 413) • Einrichten eines Onboard Administrator-Wiederherstellungsplans • Konfigurieren des Onboard Administrator-Sitzungszeitlimits • Installieren der Zertifizierungsstellenkette • Installieren von Benutzerzertifikaten auf dem lokalen Administratorkonto • Aktivieren der 2-Faktor-Authentifizierung • Anmelden bei Onboard Administrator mit der 2-Faktor-Authentifizierung
8	Aktivieren der TFA+LDAP-Authentifizierung (Aktivieren der TFA+LDAP-Authentifizierung auf Seite 422)

Die folgenden Abschnitte enthalten zudem:

- Methoden zur Angabe des Antragstellerfeldes in einer Zertifikatsignieranforderung (Methoden zur Angabe des Antragstellerfeldes in einer Zertifikatsignieranforderung auf Seite 423)
- Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen (Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen auf Seite 423)
- CLI-Beispiele für das Konfigurieren eines Benutzerkontos und von Zertifikaten (CLI-Beispiele für das Konfigurieren eines Benutzerkontos und von Zertifikaten auf Seite 425)
- Über das Internet verfügbare Informationen zu Zertifizierungsstellen und Zertifikaten (Über das Internet verfügbare Informationen zu Zertifizierungsstellen und Zertifikaten auf Seite 426)

Konfigurieren der Verzeichnisse

Dieser Abschnitt beschreibt die Konfigurationsschritte, die vor dem Erstellen der Stammzertifizierungsstelle erforderlich sind.

Erstellen eines Verzeichnisses zur Repräsentation einer jeden Zertifizierungsstelle und eines jeden Benutzers

In diesem Lernprogramm werden in dem folgenden Beispiel die anfänglichen Verzeichnisse für die Stammzertifizierungsstelle eingerichtet. Es folgt eine Beschreibung der einzelnen Verzeichnisse. In diesem und nachfolgenden Beispielen wird die Benutzereingabe auf entsprechende Eingabeaufforderungen durch **Fettdruck** ausgewiesen.

HINWEIS: Dies ist ein Lernprogramm zum Erstellen von Zertifizierungsstellen in einer einfachen Testumgebung. In einer tatsächlichen Produktionsumgebung würden sich die ZS-Server auf getrennten Servern befinden. In diesem Beispiel des Lernprogramms werden die ZS-Server durch getrennte Verzeichnisse auf einem einzelnen Server dargestellt.

```
[~/]$ mkdir –m 0755 ~/examples
[~/]$ mkdir -m 0755 \
     ~/examples/rootCA \
     ~/examples/rootCA/private \
     ~/examples/rootCA/certs \
     ~/examples/rootCA/newcerts \
     ~/examples/rootCA/crl
[~/]$ mkdir -m 0755 \
    ~/examples/level1CA \
    ~/examples/level1CA/private \
    ~/examples/level1CA/certs \
    ~/examples/level1CA/newcerts \
    ~/examples/level1CA/crl
[~/]$ mkdir -m 0755 \
    ~/examples/TestUser \
    ~/examples/TestUser/private \
    ~/examples/TestUser/certs
```

Beschreibung der Verzeichnisse

- `./private`: Der Speicherort der privaten Schlüssel. Normalerweise sollten die Berechtigungen für dieses Verzeichnis so festgelegt werden, dass der Lesezugriff auf das Stammverzeichnis (0200) oder auf das Benutzerkonto für den Webserver eingeschränkt wird. Dieses Beispiel startet mit uneingeschränktem Lese-/Schreibzugriff für alle (0755).
- `./certs`: Der Speicherort der ZS-Zertifikate.
- `./newcerts`: Der Speicherort für neue signierte Zertifikate. Sie werden im unverschlüsselter PEM-Format mit dem Dateinamensformat *Zertifikat_Seriennummer.pem* (z. B. `03.pem`) gespeichert.
- `./crl`: Der Speicherort der Zertifikatswiderrufsliste.

Ändern und Speichern einer OpenSSL-Konfigurationsdatei in jedem Zertifizierungsstellenverzeichnis

Die OpenSSL-Konfigurationsdatei (`openssl.cnf`) enthält die Standard-Verzeichnisstruktur, Namen und Optionen. Auf den meisten Linux-Auslieferungen befindet sich eine `openssl.cnf`-Standarddatei in `/etc/pki/tls`, wie im folgenden Beispiel veranschaulicht.

```
[~/examples]$ cp -v /etc/pki/tls/openssl.cnf ~/examples/
```

Ändern der Standardverzeichnisse

In diesem Beispiel wird eine Änderung für alle Zertifizierungsstellen und Benutzer vorgenommen. Diese Datei kann als Vorlage für andere Verzeichnisse dienen.

```
#####################################################################
[ CA_default ]

dir       = .  # CHANGE from "../../CA" # Everything is stored here
certs      = $dir/certs      # Issued certs are stored here
```

Erstellen einer Stammzertifizierungsstelle

Dieser Abschnitt beschreibt die Schritte zum Erstellen einer Stammzertifizierungsstelle.

Kopieren der OpenSSL-Konfigurationsdatei in das Verzeichnis der Stammzertifizierungsstelle

Kopieren Sie die Datei `openssl.cnf` in das Verzeichnis der Stammzertifizierungsstelle (in diesem Beispiel `rootCA`):

```
[~/examples]$ cp ~/examples/openssl.cnf ~/examples/rootCA/openssl-rootCA.cnf
[~/examples]$ cd ~/examples/rootCA
```

Erstellen des Zertifikats und privaten Schlüssels

Erstellen Sie den Schlüssel und das Zertifikat der Stammzertifizierungsstelle (`rootCA-private.key` und `rootCA.crt`). Im folgenden Beispiel werden als Schlüssellänge 2048 und als Hash-Signatur-Algorithmus SHA256 festgelegt. Geben Sie bei entsprechender Aufforderung eine sichere Passphrase ein. Bei Verwendung der Option `-nodes` kann die Passphrase weggelassen werden. Wenn Sie zur Eingabe eines Landes, Bundesstaates, Ortes usw. aufgefordert werden, können Sie durch Eingabe eines Punktes („.“), wie unten gezeigt, ein leeres Feld angeben.

```
[~/examples/ rootCA]$ openssl req -config ./openssl-rootCA.cnf -newkey
\rsa:2048 -x509 -extensions v3_ca -keyout private/rootCA-private.key -out
\certs/rootCA.crt -days 1825 -sha256 -nodes
Generating a 2048 bit RSA private key
.................+++
............+++
writing new private key to 'private/rootCA-private.key'
```

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: .
State or Province Name (full name) [Berkshire]: .
Locality Name (eg, city) [Newbury]: .
Organization Name (eg, company) [My Company Ltd]: .
Organizational Unit Name (eg, section) []: .
Common Name (eg, your name or your server's hostname) []: My Root CA
Email Address []: .

[~/examples/rootCA]$ ]$ ls -l private/ certs/
certs/:
total 4
-rw-rw-r-- 1 xxx 1314 Nov 10 08:11 rootCA.crt

private/:
total 4
-rw-rw-r-- 1 xxx 1675 Nov 10 08:11 rootCA-private.key
```

Um die Richtigkeit des neu erstellten Zertifikats zu überprüfen, zeigen Sie das Zertifikat durch Eingabe des im folgenden Beispiel gezeigten Befehls an:

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt -text
```

Bei einem selbstsignierten Stammzertifikat müssen die Felder `-issuer` und `-subject` übereinstimmen. Um sicherzustellen, dass sie übereinstimmen, zeigen Sie mit dem folgenden Befehl nur die Felder `-issuer` und `-subject` an:

```
[~/examples/rootCA]$ openssl x509 -in certs/rootCA.crt \
  -noout -issuer -subject
```

Erstellen einer kombinierten PEM-Datei aus einem privaten Schlüssel und einem Zertifikat

Eine kombinierte PEM-Datei aus einem privaten Schlüssel und einem Zertifikat ist erforderlich, wenn die Zertifizierungsstelle andere Zertifikate quersigniert. Auf die Datei wird von der OpenSSL-

Konfigurationsdatei verwiesen. Die folgenden Befehle ändern des Standardverzeichnis und erstellen Sie die kombinierte PEM-Datei `cakey.pem` aus privatem Schlüssel und Zertifikat:

```
[ ]$ cd ~/examples/rootCA

[ rootCA]$ cat private/rootCA-private.key certs/rootCA.crt > private/
cakey.pem
```

Erstellen untergeordneter Zertifizierungsstellen

Dieser Abschnitt beschreibt die Schritte zum Erstellen von Serverzertifikaten, die von einer anderen Zertifizierungsstelle ausgegeben (signiert) werden.

Erstellen der Verzeichnisse für die untergeordnete Zertifizierungsstelle

Sofern noch nicht vorhanden, erstellen Sie die Verzeichnisstruktur für die Datenbank der untergeordneten Zertifizierungsstelle, wie im folgenden Beispiel veranschaulicht:

```
[~/]$ mkdir -m 0755 \
   ~/examples/level1CA \
   ~/examples/level1CA/private \
   ~/examples/level1CA/certs \
   ~/examples/level1CA/newcerts \
   ~/examples/level1CA/crl
```

Kopieren Sie die geänderte Datei `openssl.cnf` in das Arbeitsverzeichnis, wie veranschaulicht:

```
[~/examples]$ cp -v openssl.cnf level1CA/

`openssl.cnf' -> `level1CA/openssl.cnf'
```

Bereitstellen von x509-Zertifikatinformationen

Ein Zertifikat enthält zahlreiche Datenelemente, die das Zertifikat beschreiben. Die Daten können auf eine entsprechende Aufforderung manuell eingegeben oder automatisch über eine OpenSSL-Konfigurationsdatei bereitgestellt werden. Das folgende Beispiel veranschaulicht, wie eine OpenSSL-Konfigurationsdatei über ein Skriptdatei erstellt wird.

```
#!/bin/sh

#

cat << _end_marker_ > openssl-level1CA.cnf

[ req ]

distinguished_name=req_DN

attributes=req_attr

prompt=no

[ req_DN ]

CN=level1CA

C=US
```

```
ST=TX

L=Houston

O=Development

subjectAltName=otherName:Gorilla

OU=Jungle

emailAddress=george@theJungle.com

surname=.

givenName=Frederick

initials=FGG

# dnQualifier=

name=George of the Jungle

[ req_attr ]

# challengePassword=

# unstructuredName=

_end_marker_
```

Erstellen einer Zertifikatsignieranforderung und eines neuen Serverschlüssels

Dieser Schritt erstellt einen neuen Schlüssel (`-newkey`) und eine Zertifikatsignieranforderung, die an eine Zertifizierungsstelle gesendet werden kann. Der neue private Schlüssel wird am Speicherort `keyout` gespeichert. Die Zertifikatsignieranforderung wird mit dem Parameter `-out` als Abbild gesichert. Zur Vereinfachung wird die Option `-nodes` verwendet, so dass kein Schutz durch eine Passphrase gewährt werden muss.

```
[~/examples/level1CA]$ openssl req -config ./openssl-level1CA.cnf -newkey
rsa:2048 -sha256 -keyout \ ./private/level1CA-private.key -nodes -out ./
temp-level1CA.csr
```

Erstellen einer Zertifikatsignieranforderung ohne neuen Schlüssel (optional)

Erstellen Sie die Zertifikatsignieranforderung ohne neuen privaten Schlüssel, wie in diesem Beispiel veranschaulicht:

```
[~/examples/level1-ca]$ openssl req -config ./openssl-level-1-ca.cnf \

-new -key ./level-1-CA-private.key -nodes -out ./level-1-CA.csr
```

Anzeigen des privaten Schlüssels

Verwenden Sie zur Ansicht des privaten Schlüssels den im folgenden Beispiel gezeigten Befehl:

```
[~/examples/level1CA]$ openssl rsa -in ./private/level1CA-private.key -
text
```

Signieren der level1CA-Zertifikatsignieranforderung mit dem Stamm-ZS-Schlüssel

Nachdem (im vorherigen Schritt) eine Zertifikatsignieranforderung erstellt wurde, muss sie von einer eingerichteten Zertifizierungsstelle in der Zertifikatkette signiert werden. Bei der ersten Signieranforderung (wenn nur die Stammzertifizierungsstelle vorhanden ist) muss die Zertifikatsignieranforderung von der Stammzertifizierungsstelle signiert werden. Nachfolgende Zertifikatsignieranforderungen können von Zertifizierungsstellen auf niedrigerer Ebene signiert werden, sofern sie dazu berechtigt sind.

In diesem Beispiel signiert die Stammzertifizierungsstelle die Zertifikatsignieranforderung der ersten Ebene (`level-1-CA.csr`).

1. Öffnen Sie die Zertifizierungsstelle, die die Anforderung signieren wird, und zeigen Sie dann die Zertifikatsignieranforderung an, um sicherzustellen, dass sie wirklich signiert werden soll:

   ```
   [ ]$ cd ~/examples/rootCA/

   [ rootCA]$ openssl req -in ../level1CA/temp-level1CA.csr -noout -text
   ```

2. Führen Sie den folgenden einmaligen Konfigurationsschritt durch:

   ```
   [ rootCA]$ echo '01' > serial

   [ rootCA]$ touch index.txt
   ```

3. Nachdem sichergestellt wurde, dass die Zertifikatsignieranforderung signiert werden soll, nehmen Sie die Signierung durch Ausgabe des folgenden Befehls vor:

   ```
   [~/examples/rootCA]$ openssl ca \

    -config openssl-rootCA.cnf \

    -extensions v3_ca -policy policy_anything \

    -in ../level1CA/temp-level1CA.csr \

    -cert certs/rootCA.crt \

    -default_md sha256 \

    -key private/rootCA-private.key
   ```

   Das signierte Zertifikat wird in `./certs/{`*serialNumber*`}.pem` geschrieben. Die Dateien `serial` und `index.txt` wurden aktualisiert.

4. Installieren Sie das Zertifikat auf dem ZS-Server der ersten Ebene und geben Sie die entsprechende Seriennummer an (in diesem Beispiel ist die Seriennummer `01`).

   ```
   [ ~]$ cp ~/examples/rootCA/newcerts/01.pem ~/examples/level1CA/certs/
   level1CA.pem
   ```

Erstellen von Benutzerschlüsseln und Zertifikatsignieranforderungen

Die Schritte zum Erstellen eines neuen Benutzerschlüssels und einer Zertifikatsignieranforderung unterscheiden sich nur in der Angabe eines anderen Typs von den Schritten zum Erstellen einer Zertifikatsignieranforderung für eine Zertifizierungsstelle.

Erstellen eines Verzeichnisses für die Datenbank der Benutzerschlüssel und Zertifikatsignieranforderungen

Sofern nicht bereits vorhanden, erstellen Sie die Verzeichnisstruktur für die Datenbank der Benutzerschlüssel und Zertifikatsignieranforderungen:

```
[~/]$ mkdir -m 0755 \
   ~/examples/TestUser \
   ~/examples/TestUser/private \
   ~/examples/TestUser/certs
```

Kopieren Sie die geänderte Datei `openssl.cnf` in das Arbeitsverzeichnis:

```
[~/examples]$ cp -v ~/examples/openssl.cnf ~/examples/TestUser/
`~/examples/openssl.cnf' -> `~/examples/TestUser/openssl.cnf'
```

Bereitstellen von x 509-Benutzerzertifikatinformationen

Die Daten können auf eine entsprechende Aufforderung manuell eingegeben oder automatisch über eine OpenSSL-Konfigurationsdatei bereitgestellt werden. Die Standardkonfigurationsdatei ist ausreichend.

Erstellen einer Benutzer-Zertifikatsignieranforderung und eines neuen Serverschlüssels

Dieser Schritt erstellt einen neuen Schlüssel (`-newkey`) und eine Zertifikatanforderung für einen Benutzer. Das daraufhin angezeigte Zertifikat schließt das Antragstellerfeld (`-subj`) ein. Das Antragstellerfeld kann in der OpenSSL-Befehlszeile als einzelner Parameter angegeben oder aus verschiedenen Feldern in der Datei `openssl.cnf` aufgefüllt werden. (Weitere Informationen finden Sie unter „Methoden zum Angeben des Antragstellerfeldes in einer Zertifikatsignieranforderung“ (Methoden zur Angabe des Antragstellerfeldes in einer Zertifikatsignieranforderung auf Seite 423).) Die Zertifikatsignieranforderung wird in die durch den Parameter `-out` angegebene Datei geschrieben. Im folgenden Beispielsbefehl wird das Antragstellerfeld als einzelner Parameter angegeben, und die Zertifikatsignieranforderung wird in `./temp-test-user.csr` geschrieben.

```
[~/examples/TestUser]$ openssl req \
-subj "/O=Hewlett-Packard Company/OU=Employment Status - Employees/OU=VPN-WEB-H/CN=Jonathan Smith/emailAddress=jonathan.smith@hp.com" \
-config ./openssl.cnf \
-newkey rsa:2048 -sha256 \
-keyout ./private/test-user-private.key \
-nodes \
-out ./temp-test-user.csr
```

Zeigen Sie die Zertifikatsignieranforderung an und stellen Sie sicher, dass sie signiert werden soll. Der folgende Befehl zeigt die Zertifikatsignieranforderung an:

```
[ ]$ openssl req -in ./temp-test-user.csr -text
```

Signieren der Benutzer-Zertifikatsignieranforderung mit dem level1CA-Schlüssel

So verfahren Sie zum Signieren und Konfigurieren eines Benutzerzertifikats:

1. Signieren Sie die Benutzer-Zertifikatsignieranforderung wie im vorherigen Beispiel mit dem Schlüssel `level1CA`:

   `[ ]$`**cd ~/examples/level1CA/**

2. Zeigen Sie die Zertifikatsignieranforderung an und stellen Sie sicher, dass sie signiert werden soll. Der folgende Befehl zeigt die Zertifikatsignieranforderung an:

   `[ level1CA]$`**openssl req -in ../TestUser/temp-test-user.csr -text**

3. Es ist wichtig, anzugeben, wie das Benutzerzertifikat verwendet werden kann. Verwenden Sie hierzu x509-Erweiterungen. (Weitere Informationen zu x509-Erweiterungen finden Sie auf der OpenSSL-Website (http://www.openssl.org/docs/apps/x509v3_config.html#).) Der Unterschied zwischen einem Serverzertifikat und einem Benutzerzertifikat besteht in den Berechtigungen, die die Zertifizierungsstelle dem Zertifikat zuweist. So wird ein ZS-Zertifikat in der Regel als SSL-Server verwendet, während ein Benutzerzertifikat als SSL-Client und Smart Card-Anmeldung verwendet werden muss.

   Zur Angabe der Erweiterungen ändern Sie wie im folgenden Beispiel veranschaulicht den Abschnitt `[ user_cert ]` in der Datei `openssl.cnf`. Kommentieren Sie die Zeilen `nsCertType` und `keyUsage` wie gezeigt aus. Die geänderten Zeilen werden in Fettdruck dargestellt.

```
[ usr_cert ]

# These extensions are added when 'ca' signs a request.

# This goes against PKIX guidelines but some CAs do it and some
software

# requires this to avoid interpreting an end user certificate as a CA.

basicConstraints=critical, CA:FALSE

# Here are some examples of the usage of nsCertType. If it is omitted

# the certificate can be used for anything *except* object signing.

# This is OK for an SSL server.

# nsCertType          = server

# For an object signing certificate this would be used.

# nsCertType = objsign

# For normal client use this is typical

nsCertType = client, email # Uncomment this line

# and for everything including object signing:

# nsCertType = client, email, objsign
```

```
# This is typical in keyUsage for a client certificate.
# Uncomment this line:
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment

# If extendedKeyUsage is specified, it MUST include all three items
# to be used for Two-Factor authentication.
#   Client Authentication (1.3.6.1.5.5.7.3.2)
#   Code Signing (1.3.6.1.5.5.7.3.3)
#   Smart Card Login (1.3.6.1.4.1.311.20.2.2)
#
extendedKeyUsage=clientAuth,codeSigning,1.3.6.1.4.1.311.20.2.2

# This will be displayed in Netscape's comment listbox.
nsComment = "OpenSSL Generated Certificate"

# PKIX recommendations harmless if included in all certificates.
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

# This stuff is for subjectAltName and issuerAltname.
# Import the email address.
# subjectAltName=email:copy
# An alternative to produce certificates that aren't
# deprecated according to PKIX.
# subjectAltName=email:move

# Copy subject details
# issuerAltName=issuer:copy

# For testing purposes we will just use some well known CR
nsCaRevocationUrl = http://onsitecrl.verisign.com/
HewlettPackardCompanyITInfrastructure/LatestCRL.crl
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
```

4. Signieren Sie die Zertifikatanforderung wie im folgenden Beispiel:

```
[level1CA]$ openssl ca -config ./openssl.cnf -extensions usr_cert \-
policy policy_anything -in ../TestUser/temp-test-user.csr -cert \
certs/level1CA.pem -md sha256 -keyfile private/level1CA-private.key
```

5. Geben Sie zur Anzeige der Ergebnisse den folgenden Befehl aus:

   ```
   [ level1CA]$ openssl x509 -in newcerts/07.pem -noout -text
   ```

6. Zum Aktivieren der Zertifikatverwendung in Smart Cards muss das Feld `keyUsage` den Parameter `sslAuth` enthalten. Außerdem muss das Feld `extendedKeyUsage`, sofern vorhanden, die Client-Authentifizierung, Codesignierung und Smart Card-Anmeldung angeben. Weitere Informationen finden Sie unter „Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen“ (Fehlerbehebung von TFA- und LDAP-Authentifizierungsprobleme auf Seite 423).

7. Übergeben Sie das öffentliche Zertifikat mit dem folgenden Befehl dem Benutzer:

   ```
   [ TestUser]$cp -v ~/examples/level1CA/newcerts/07.pem ~/examples/Test/User/certs/test-user.pem

   `../level1CA/newcerts/06.pem' -> `certs/test-user.pem'
   ```

8. Kombinieren Sie das öffentliche Zertifikat und den öffentlichen Schlüssel in einer PKCS #12 `.pem`-Datei, indem Sie ein PKCS #12-Zertifikat erstellen und ein Kennwort (PIN) für das Zertifikat bereitstellen. Der Benutzer wird zur Eingabe des Kennwortes (PIN) aufgefordert. Dieses Kennwort schützt den im PKCS #12-Zertifikat enthaltenen Schlüssel.

   ```
   [ ]$cd ~/examples/TestUser

   [ TestUser]$openssl pkcs12 -export -in certs/test-user.pem -inkey \private/test-user-private.key -out private/test-user-private.p12
   ```

Überprüfen von Zertifikaten

Verfahren Sie zum Überprüfen der Zertifikate wie folgt.

1. Um die Zertifikate zu überprüfen, verwenden Sie die im folgenden Beispiel gezeigten Befehle:

   ```
   [ examples]$mkdir CA

   [ examples]$cp -v rootCA/certs/rootCA.crt CA/CA.pem
   `rootCA/certs/rootCA.crt' -> `CA/CA.pem'

   [ examples]$cat level1CA/certs/level1CA.pem >> CA/CA.pem

   [ examples]$openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver./level1CA/certs/level1CA.pem
   ./level1CA/certs/level1CA.pem: OK
   ```

2. Stellen Sie wie im folgenden Befehl veranschaulicht sicher, dass das Benutzerzertifikat nicht für SSL-Serverzwecke verwendet werden kann:

   ```
   [examples]$openssl verify -CAfile CA/CA.pem -verbose -purpose sslserver ./TestUser/certs/test-user.pem

   ./TestUser/certs/test-user.pem: /O=Hewlett-Packard Company/
   OU=EmploymentStatus - Employees/OU=VPN-WEB-H/CN=JonathanSmith/
   emailAddress=jonathan.smith@hp.com
   ```

```
error 26 at 0 depth lookup:unsupported certificate purpose
OK
```

Stellen Sie sicher, dass das Benutzerzertifikat für SSL-Client-Zwecke verwendet werden kann:

```
[user1@user1-station examples]$openssl verify -CAfile CA/CA.pem -verbose -purpose sslclient ./TestUser/certs/test-user.pem
./TestUser/certs/test-user.pem: OK
```

Speichern eines Benutzerzertifikats auf einer Smart Card oder einem Browser

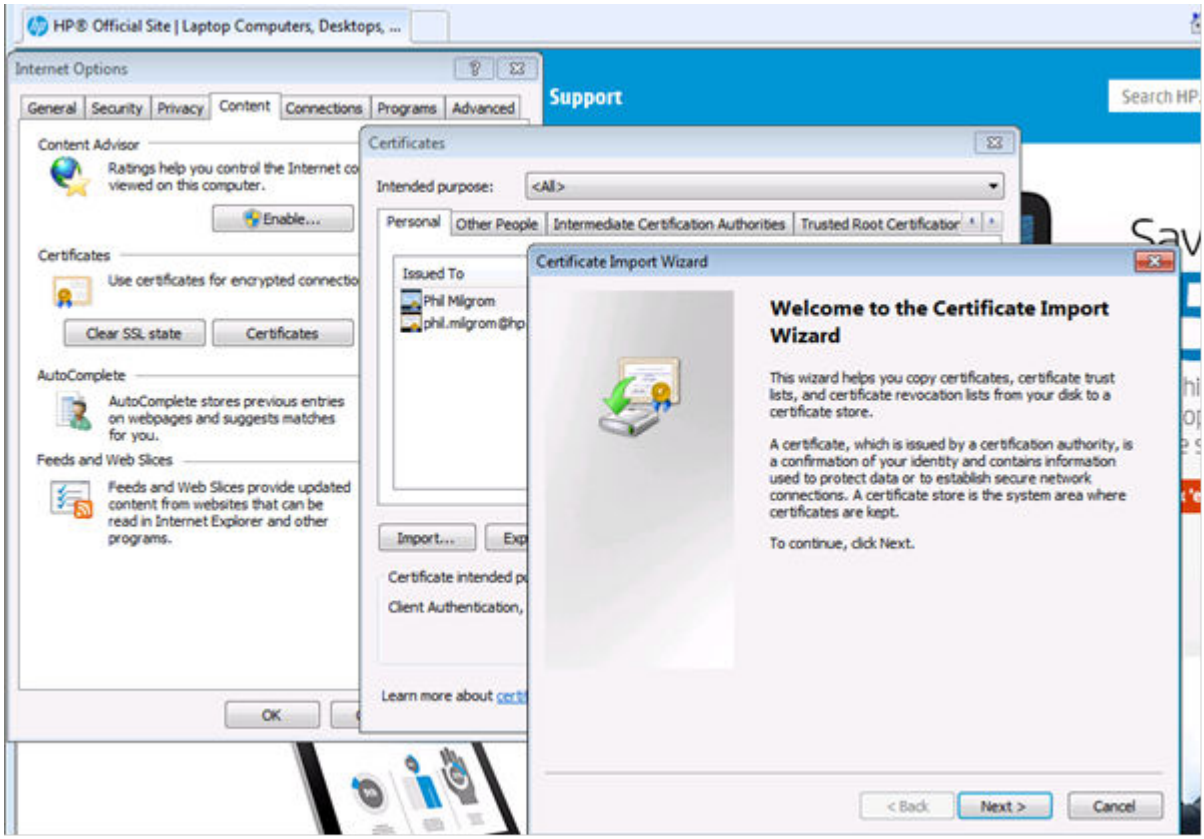
In diesem Abschnitt wird beschrieben, wie ein Benutzerzertifikat auf einer Smart Card oder einem Browser gespeichert wird. Die Browser-Informationen in diesem Abschnitt basieren auf Microsoft Internet Explorer.

Microsoft Internet Explorer unterstützt keine PEM-formatierten Dateien. Erstellen Sie mit einem Befehl wie dem Folgenden ein `.p12`-Zertifikat, das die privaten und öffentlichen Schlüssel enthält:

```
[ TestUser]$ openssl pkcs12 -export -in certs/test-user.pem -inkey private/test-user-private.key -out private/test-user-private.p12
```

Verfahren Sie wie folgt, um das `.p12`-Zertifikat mit Internet Explorer 8 zu installieren:

1. Rufen Sie den Internetzertifikat-Assistenten von Internet Explorer durch Klicken auf **Extras>Internetoptionen>Inhalt>Zertifikate** auf:

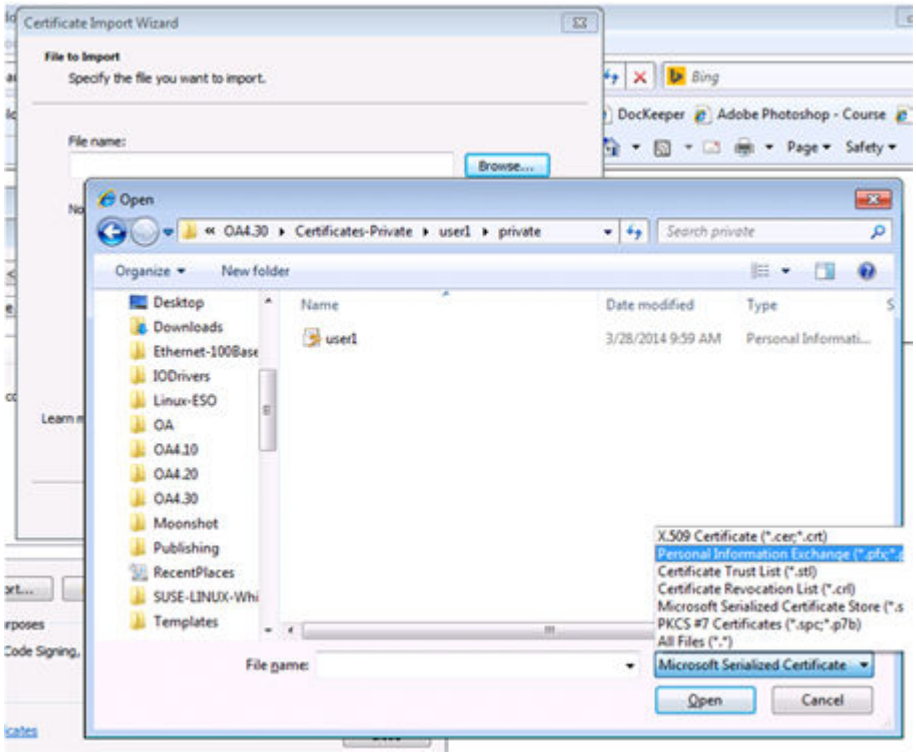

HP® Official Site | Laptop Computers, Desktops, ...
Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Content Advisor
Ratings help you control the Internet co
viewed on this computer.
Enable...
Certificates
Use certificates for encrypted connectio
Clear SSL state
Certificates
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.
OK
Support
Search HP
Certificates
Intended purpose:
<All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Issued To
Phil Milgrom
phil.milgrom@hp
Import...
Certificate intended p
Client Authentication,
Learn more about certi
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

2. Klicken Sie auf **Weiter**.

3. Klicken Sie auf **Durchsuchen...**.

   a. Suchen Sie das Verzeichnis mit der `.p12`-Zertifikatdatei.

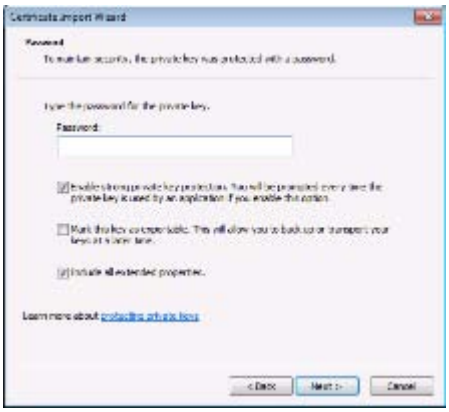
   b. Ändern Sie den Dateityp in `Personal Information Exchange (.p12)`.



   c. Wählen Sie die entsprechende `.p12`-Zertifikatdatei aus.

4. Wählen Sie die Datei `.p12` aus und klicken Sie auf **Weiter**.

5. Geben Sie das Kennwort ein, das beim Erstellen der PKCS #12-Datei angegeben wurde (siehe „Signieren der Benutzer-Zertifikatsignieranforderung mit dem level1CA-Schlüssel“ (Signieren der Benutzer-Zertifikatsignieranforderung mit dem level1CA-Schlüssel auf Seite 408)) und klicken Sie auf **Weiter**. (Akzeptieren Sie die Standardwerte der Kontrollkästchen.)



6. Der Bildschirm „Zertifikatspeicher“ wird angezeigt. Klicken Sie auf **Weiter**.

7. Um den Assistenten-Installationsvorgang (Importvorgang) abzuschließen, klicken Sie auf **Fertig stellen**.

8. Das nächste Fenster meldet, dass eine Anwendung derzeit ein geschütztes Element erstellt und die Sicherheitsebene für das betreffende Element festgelegt wird. Klicken Sie auf **OK**.
9. Wenn der Assistent meldet, dass der Importvorgang erfolgreich war, klicken Sie auf **OK**.

Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung anhand lokaler Konten

Dieser Abschnitt zeigt anhand eines Beispiels, wie Onboard Administrator konfiguriert wird, so dass die 2-Faktor-Authentifizierung erzwungen wird.

Einrichten eines Onboard Administrator-Wiederherstellungsplans

HP empfiehlt, vor dem Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung einen Wiederherstellungsplan aufzustellen. Sollte während der Konfiguration etwas falsch laufen, kann die Onboard Administrator-Konfiguration durch Zugriff auf das USB-Schlüssellaufwerk entweder über den seriellen Port oder das Insight Display-Bedienfeld wiederhergestellt werden. Beide Methoden erfordern physischen Zugriff auf das Onboard Administrator-Modul.

HINWEIS: Falls eine LCD-PIN konfiguriert (und vergessen) wurde, lokale Benutzerkonten deaktiviert wurden oder TFA falsch konfiguriert wurde, besteht die einzige Möglichkeit zur Wiederherstellung über einen seriellen Port.

Onboard Administrator muss am häufigsten wiederhergestellt werden, wenn LDAP mit lokalen Konten konfiguriert wurde, die deaktiviert wurden, oder wenn die 2-Faktor-Authentifizierung ohne Zertifikatzugriff (`keyUsage`) konfiguriert wurde.

Wiederherstellen über das Insight Display und einen USB-Schlüssel

Um Onboard Administrator über einen USB-Schlüssel wiederherzustellen, erstellen Sie auf dem USB-Schlüssel eine Konfigurationsdatei zum Wiederherstellen der erforderlichen Einstellungen. Die Datei kann so konfiguriert werden, dass entweder nur die Einstellungen zum Wiederherstellen des Zugriffs zurückgesetzt werden oder dass die Werkseinstellungen vollständig wiederhergestellt werden:

- `GAIN_ACCESS.CFG` (nur das Notwendigste zum Wiederherstellen des Zugriffs zurücksetzen):

  ```
  DISABLE TWOFACTOR

  DISABLE LDAP

  SET USER PASSWORD "Administrator" "My.Password123"
  ```

- `SET_FACTORY.CFG` (Werkseinstellungen wiederherstellen):

  ```
  SET FACTORY
  ```

So stellen Sie eine Konfiguration wieder her:

1. Stecken Sie den USB-Schlüssel mit der Konfigurationsdatei in den USB-Port des Onboard Administrators.
2. Navigieren Sie mittels der Insight Display-Anzeige zum Hauptmenü, wählen Sie **USB Key Menu** (USB-Schlüsselmenü), und klicken Sie auf **OK**.
3. Wählen Sie **Restore Configuration** (Konfiguration wiederherstellen), und klicken Sie auf **OK**.
4. Wählen Sie die ausgewählte Konfigurationsdatei aus und klicken Sie dann auf **OK**.
5. Der Bildschirm „Confirm Operation“ (Vorgang bestätigen) wird angezeigt. Klicken Sie auf **OK**.

Wiederherstellung über die serielle Konsole

Um Onboard Administrator über den seriellen Port wiederherzustellen, verfahren Sie wie folgt:

1. Stellen Sie sicher, dass Sie über die entsprechenden Kabel und die entsprechende Software zum Herstellen einer Verbindung zum seriellen Port des Onboard Administrator-Moduls verfügen. Die serielle Standardverbindungseinstellung ist 9600, 8, N,1. Weitere Informationen finden Sie unter „Wiederherstellen des Administrator-Kennworts“ (Wiederherstellen des Administratorkennworts auf Seite 15).
2. Drücken und halten Sie die Taste **Reset** fünf Sekunden lang gedrückt.
3. Wenn Sie an der seriellen Konsole zur Auswahl von „Flash Recovery“ (Flash-Wiederherstellung) oder „Reset Password“ (Kennwort zurücksetzen) aufgefordert werden, drücken Sie die Taste **L** für „Lost Password“ (Verlorenes Kennwort).

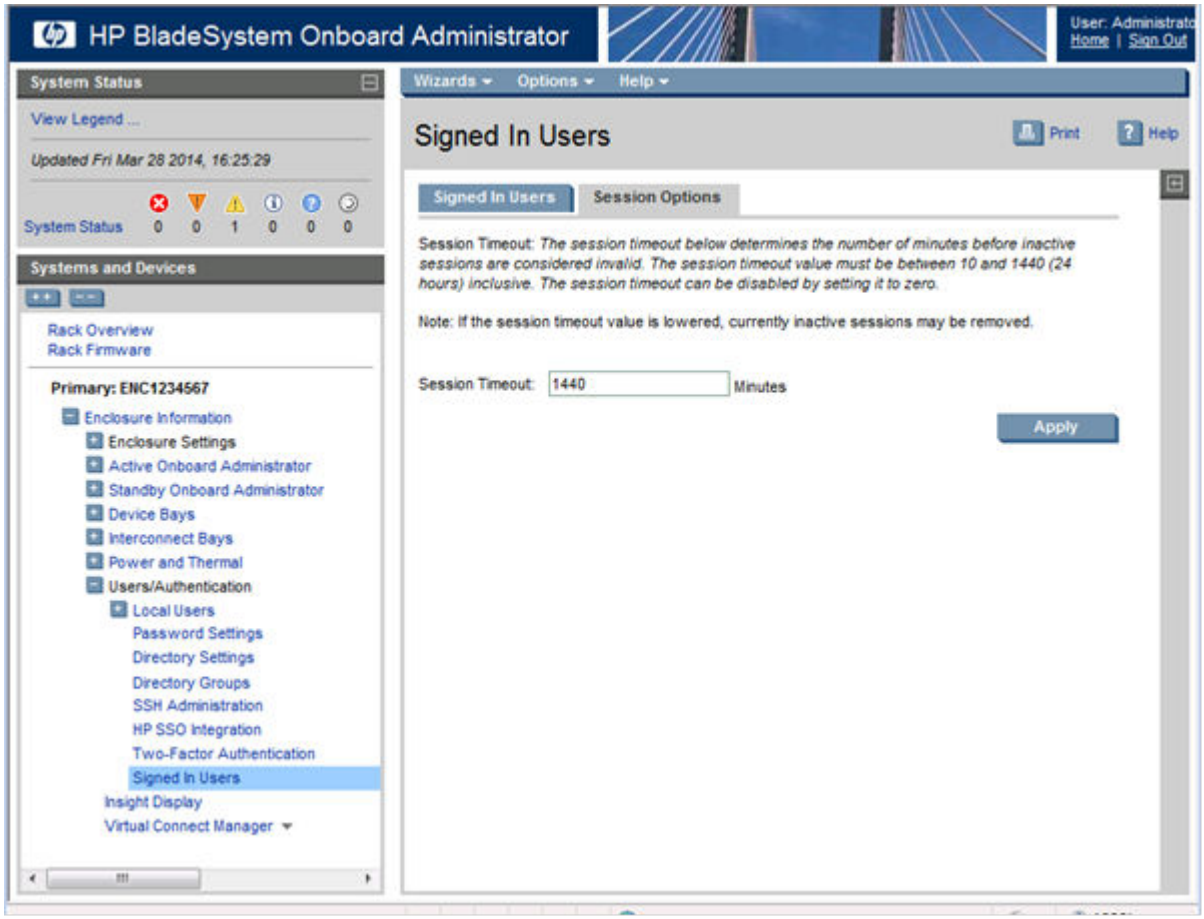
   Die Konsole zeigt das integrierte Kennwort des Administratorkontos an und lokale Anmeldungen sind aktiviert.

Konfigurieren des Onboard Administrator-Sitzungszeitlimits

Standardmäßig tritt eine Zeitüberschreitung auf, wenn eine Benutzersitzung einen Tag (1440 Minuten) lang inaktiv ist. Verringern Sie diese Einstellung auf einen Wert, der für Ihre Sicherheitsrichtlinie geeignet ist. Zu Testzwecken können Sie das Zeitlimit auf den Mindestwert von 10 Minuten einstellen. Das eingestellte Zeitlimit kann über die Onboard Administrator-GUI oder einen CLI-Befehl geändert werden. Gültige Werte für das Zeitlimit sind 0 (wodurch das Zeitlimit deaktiviert wird) oder eine Ganzzahl im Bereich von 10 bis 1440.

Verwenden der grafischen Benutzeroberfläche (GUI)

1. Navigieren Sie zum Bildschirm **Signed in Users** (Angemeldete Benutzer) (**Enclosure Information (Gehäuseinformationen)>Users/Authentication (Benutzer/Authentifizierung)>Signed in Users (Angemeldete Benutzer)**) und wählen Sie die Registerkarte **Session Options** (Sitzungsoptionen).



2. Ändern Sie den Wert im Feld **Session Timeout** (Sitzungszeitlimit).
3. Klicken Sie auf **Apply** (Übernehmen).

Verwenden der Befehlszeilenschnittstelle (CLI)

Verwenden Sie den folgenden Befehl, wobei <*Zeitlimit-Wert* > die Anzahl von Minuten ist:

`SET SESSION TIMEOUT<`*Zeitlimit-Wert*`>`

Installieren der Zertifizierungsstellenkette für TFA

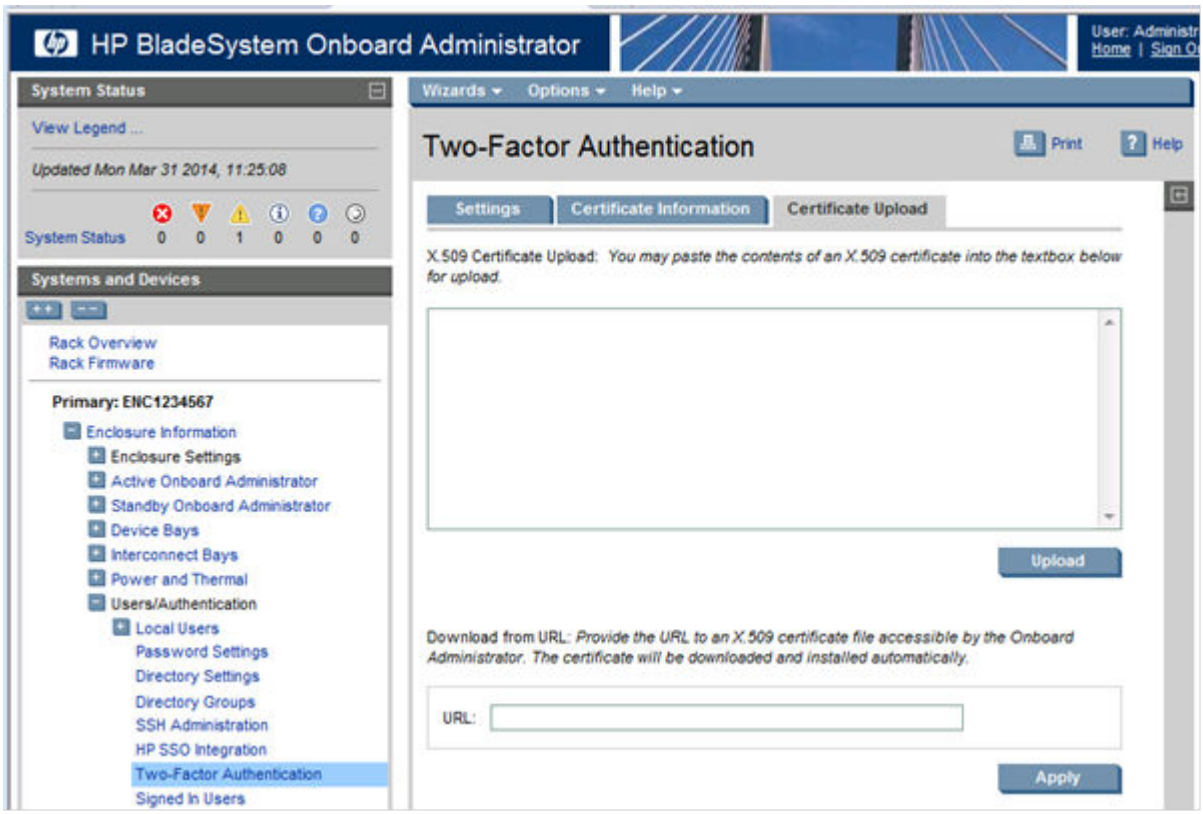
Eine Zertifikatkette besteht aus allen Zertifikaten, die zum Überprüfen des Benutzerzertifikats benötigt werden. Die Zertifikatkette beginnt mit dem Stammzertifikat, an das sich die Zertifikate aller dazwischenliegenden Zertifizierungsstellen anschließen. Jede dazwischenliegende Zertifizierungsstelle in der Kette ist der Inhaber eines Zertifikats, das von der Zertifizierungsstelle ausgegeben wurde, die sich in der Vertrauenshierarchie jeweils eine Ebene weiter oben befindet. Die Stammzertifizierungsstelle stellt sich selbst ein Zertifikat aus.

Dieser Abschnitt beschreibt, wie zwei Zertifizierungsstellen für die 2-Faktor-Authentifizierung installiert werden.

HINWEIS: Die 2-Faktor-Authentifizierung und LDAP verfügen über separate Repositories für Zertifizierungsstellen. Diese dürfen nicht miteinander verwechselt werden.

Verfahren Sie zum Installieren der ZS-Zertifikate für die 2-Faktor-Authentifizierung auf der Onboard Administrator-GUI wie folgt:

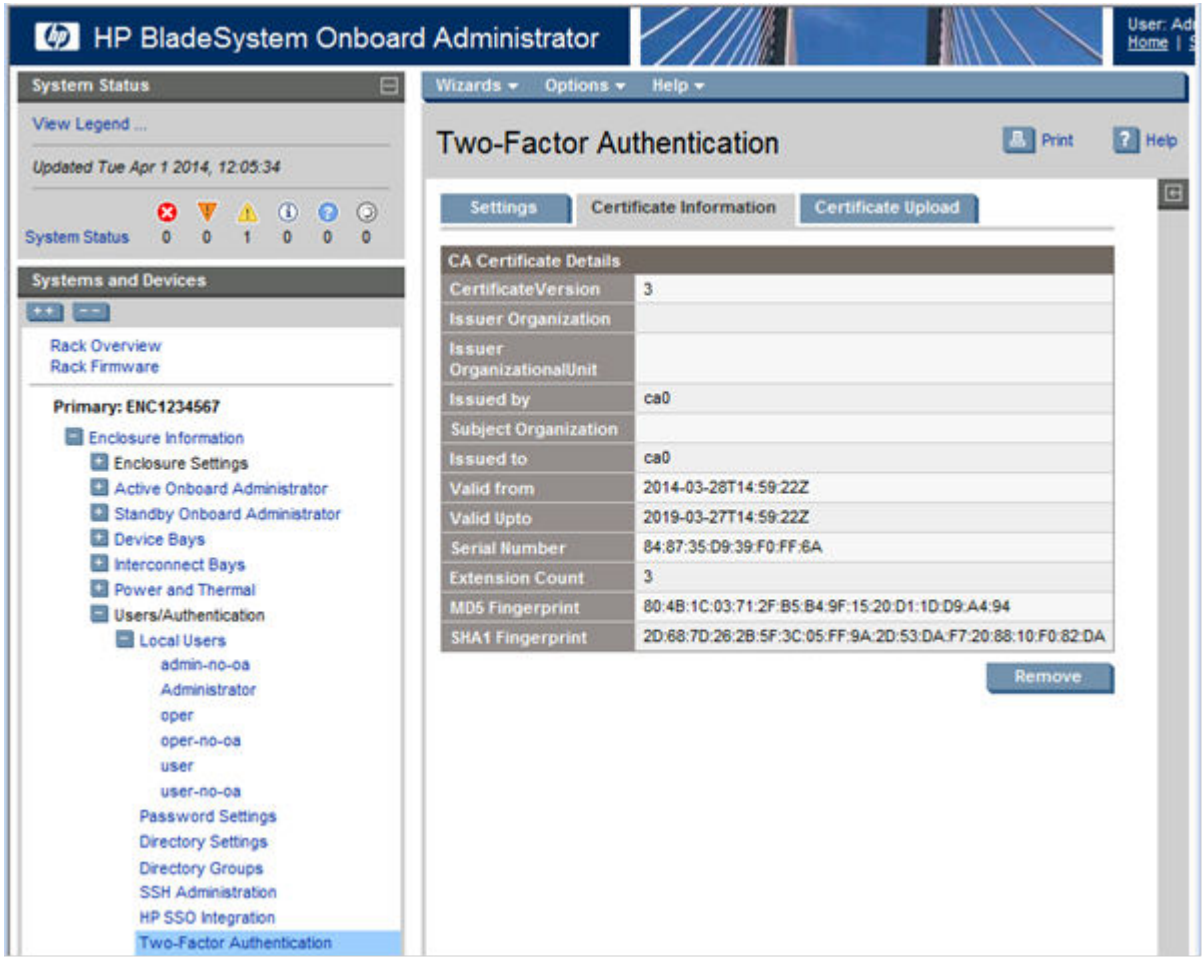
1. Navigieren Sie zum Bildschirm der 2-Faktor-Authentifizierung: **Enclosure Information (Gehäuseinformationen)>Users/Authentication (Benutzer/Authentifizierung)>Two-Factor Authentication (2-Faktor-Authentifizierung)**.
2. Klicken Sie auf die Registerkarte **Certificate Upload** (Zertifikat-Upload). Der Bildschirm **Certificate Upload** (Zertifikat-Upload) wird wie im folgenden Beispiel angezeigt.



3. Kopieren Sie das Zertifikat der Stammzertifizierungsstelle und fügen Sie es in das entsprechende Textfeld auf dem Bildschirm **Certificate Upload** (Zertifikat-Upload) ein. Das Zertifikat enthält Textbegrenzer für den Beginn und das Ende des Textes, wie hier veranschaulicht:

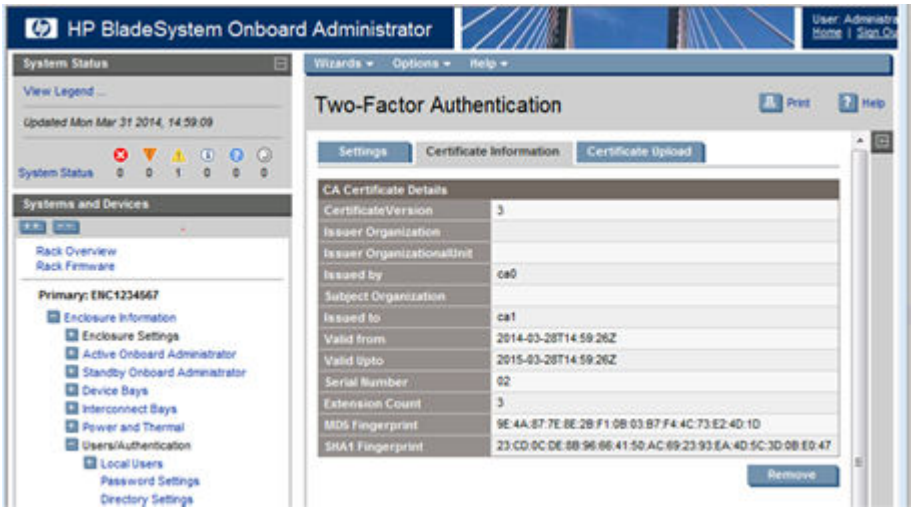
```
-----BEGIN CERTIFICATE-----

MIIDkTCCAnmgAwIBAgIJALg8cO2Ikvr8MA0GCSqGSIb3DQEBBQUAMDkxDDAKBgNV

BAMTA2NhMDEUMBIGCgmSJomT8ixkARkWBHRlc3QxEzARBgoJkiaJk/IsZAEZFgNj

.

.

.

Ob6IFCSUTKbCVT95cYTRHiSbgBYaqDXBJk3Lyjvtb7ZovmMT5dnU/w061wV5MEce

RZfXH3U=

-----END CERTIFICATE-----
```

4. Klicken Sie auf **Upload** (Hochladen). Nachdem das Zertifikat erfolgreich hochgeladen wurde, wird die Registerkarte **Certificate Information** (Zertifikatinformationen) wie in dem folgenden Beispiel angezeigt.



5. Fügen Sie eine dazwischenliegende oder abschließende Zertifizierungsstelle in die Kette ein:
   a. Kehren Sie wieder zur Registerkarte **Certificate Upload** (Zertifikat-Upload) zurück.
   b. Kopieren Sie das Zertifikat der nächsten Zertifizierungsstelle und fügen Sie es in das entsprechende Textfeld ein.

c. Klicken Sie auf **Upload** (Hochladen). Nachdem das Zertifikat erfolgreich hochgeladen wurde, wird die Registerkarte **Certificate Information** (Zertifikatinformationen) wie in dem folgenden Beispiel angezeigt (in diesem Beispiel wurde das CA1-Zertifikat von der Stammzertifizierungsstelle CA0 ausgestellt).



d. Um weitere Zertifizierungsstellen zu installieren, wiederholen Sie die Schritte a bis c für jedes dazwischenliegende Zertifikat.

CLI-Befehle für die Verwaltung von Zertifikaten

Mit den folgenden CLI-Befehlen können Sie Zertifikate hinzufügen, herunterladen, anzeigen und entfernen. Weitere Informationen finden Sie im *HP BladeSystem Onboard Administrator Befehlszeilenschnittstelle Benutzerhandbuch*.

- `ADD CA CERTIFICATE`
- `DOWNLOAD CA CERTIFICATE`
- `SHOW CA CERTIFICATE`
- `REMOVE CA CERTIFICATE`

Konfigurieren des HTTP-Proxy

Onboard Administrator benötigt möglicherweise einen Proxyserver, um Adressen zu erreichen, die zum Überprüfen eines Zertifikats oder zum Beziehen einer Zertifikatsperrliste erforderlich sind. (Eine Zertifikatsperrliste ist eine Datenbank mit Zertifikaten, die vor ihrem Ablaufdatum gesperrt wurden.) Konfigurieren Sie zu diesem Zweck mit dem folgenden Befehl den HTTP-Proxyserver auf Onboard Administrator:

`SET URB PROXY URL { <URL> }`

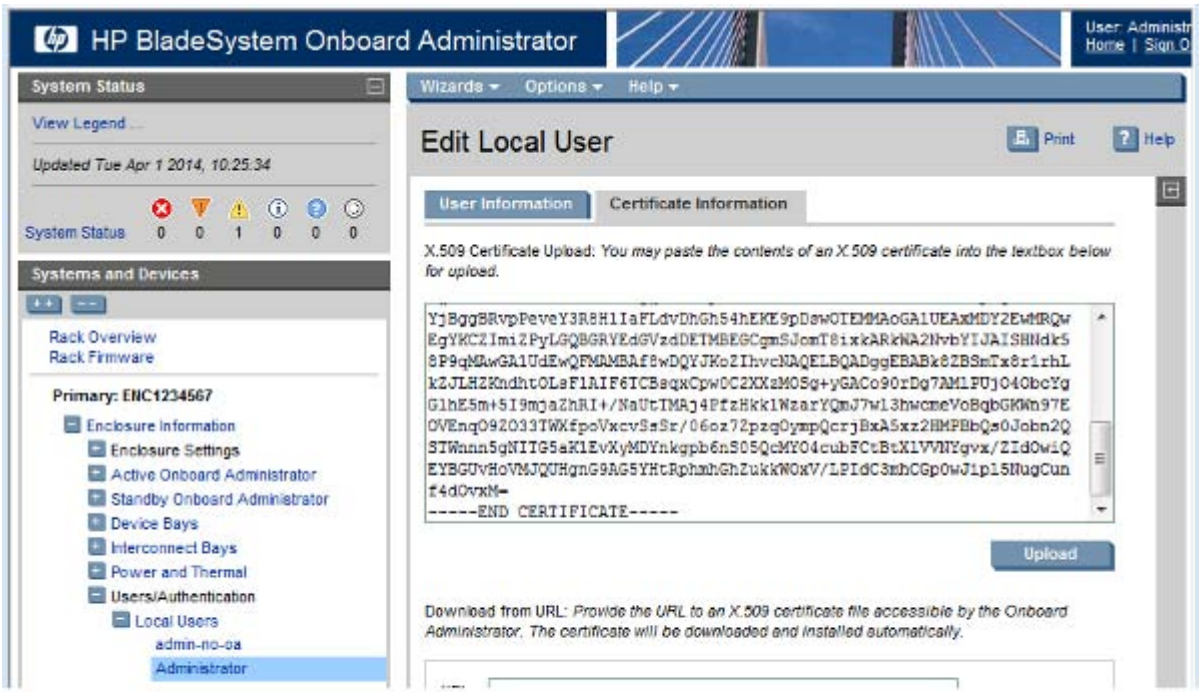
Das angegebene Kennwort kann bis zu 128 Zeichen lang sein.

Es ist nicht möglich, eine Proxy-URL über die Onboard Administrator-GUI festzulegen.

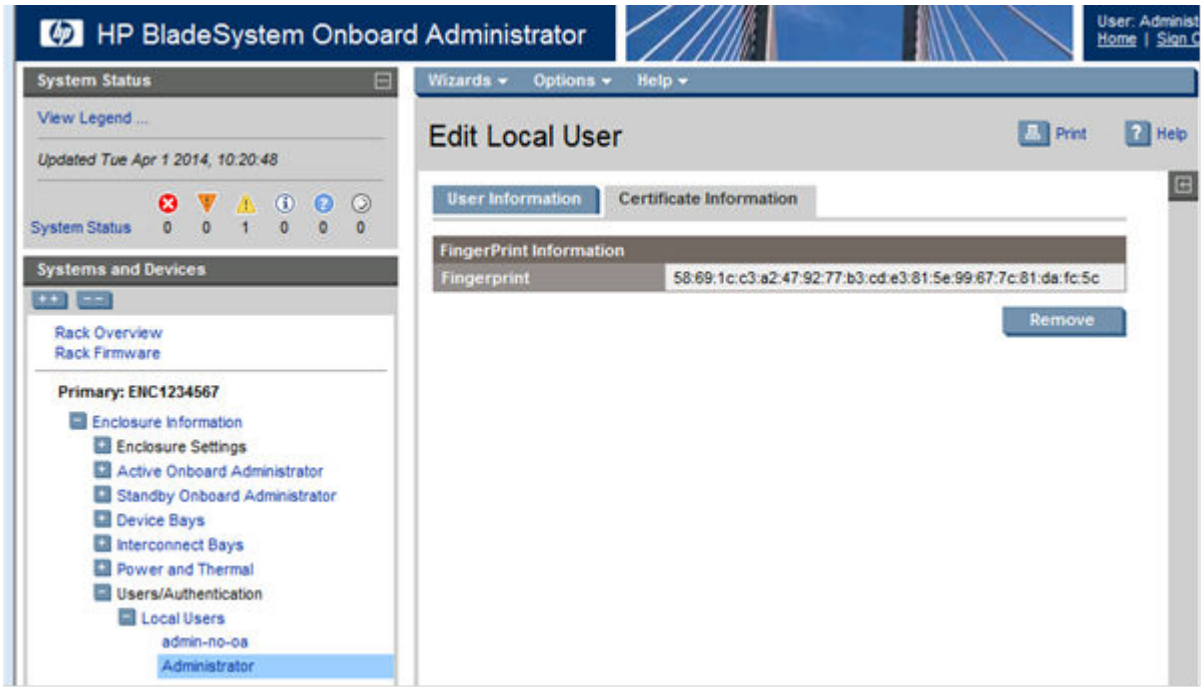
Installieren von Benutzerzertifikaten auf dem lokalen Administratorkonto

Verfahren Sie zum Installieren eines Benutzerzertifikats auf dem Onboard Administratorkonto wie folgt:

1. Navigieren Sie zum Bildschirm „Local Users Administrator“ (Administrator lokaler Benutzer („Edit Local User“ (Lokalen Benutzer bearbeiten)): **Enclosure Information (Gehäuseinformationen)>Users/Authentication (Benutzer/Authentifizierung)>Local Users (Lokale Benutzer)>Administrator**.
2. Klicken Sie auf die Registerkarte **Certificate Information** (Zertifikatinformationen). Wenn noch kein Administratorzertifikat installiert wurde, wird der Bildschirm **Certificate Information** (Zertifikatinformationen) mit einem leeren Textfeld angezeigt. Kopieren Sie das entsprechende Benutzerzertifikat und fügen Sie es wie gezeigt in das Textfeld ein.



3. Klicken Sie auf **Upload** (Hochladen). Nachdem das Zertifikat erfolgreich hochgeladen wurde, wird die Registerkarte **Certificate Information** (Zertifikatinformationen) wie im folgenden Beispiel angezeigt:



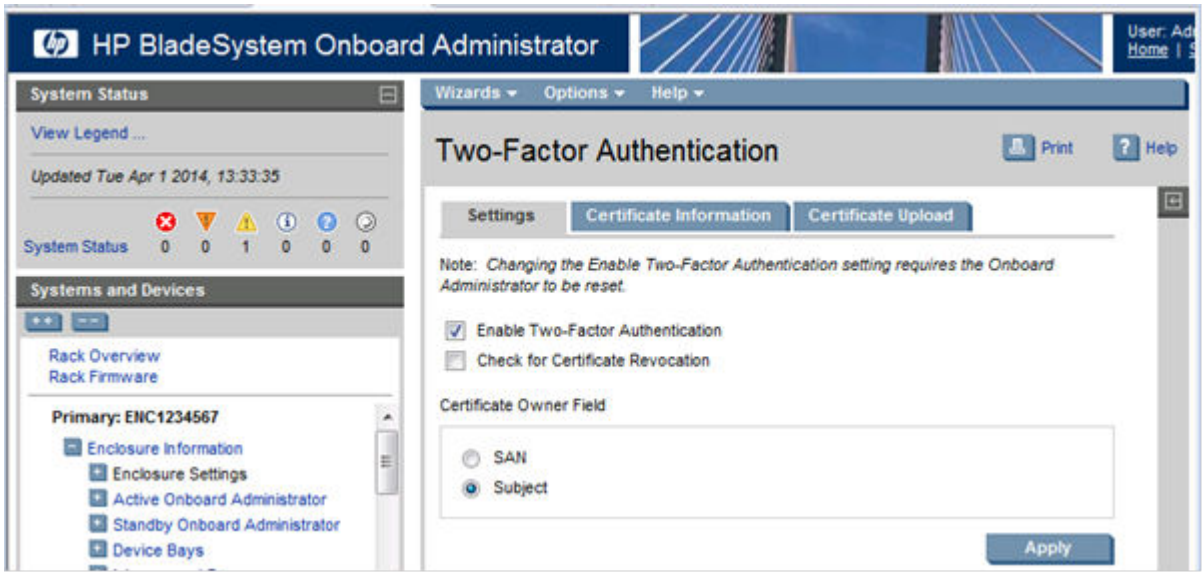
Wenn das hochgeladene Benutzerzertifikat nicht überprüft werden kann, schlagen Sie unter „Verschiedene bekannte Probleme“ (Verschiedene bekannte Probleme auf Seite 387) nach.

Aktivieren der 2-Faktor-Authentifizierung

Nachdem die ZS-Zertifikate für die 2-Faktor-Authentifizierung erfolgreich hochgeladen wurden und nachdem mindestens ein Onboard Administrator-Konto hochgeladen wurde, können Sie die 2-Faktor-Authentifizierung aktivieren:

1. Navigieren Sie zur Registerkarte **Two-Factor Authentication Settings (Einstellungen der 2-Faktor-Authentifizierung)** (klicken Sie auf **Enclosure Information (Gehäuseinformationen)>Users/Authentication (Benutzer/Authentifizierung)>Local Users (Lokale Benutzer)>Two-Factor Authentication (2-Faktor-Authentifizierung)**).

   Aktivieren Sie das Kontrollkästchen **Enable Two-Factor Authentication** (2-Faktor-Authentifizierung aktivieren), wie im folgenden Beispiel veranschaulicht. Bei Verwendung der 2-Faktor-Authentifizierung in Kombination mit LDAP geben Sie im Feld **Certificate Owner** (Zertifikateigentümer) an, ob Onboard Administrator das Feld für den alternativen Antragssteller **(SAN)** oder Feld für den Zertifikatantragsteller (**Antragsteller**) verwenden soll. Weitere Informationen zur Verwendung der 2-Faktor-Authentifizierung mit LDAP finden Sie unter „TFA +LDAP-Authentifizierung“ (auf Seite TFA+LDAP-Authentifizierung auf Seite 421)



2. Klicken Sie auf **Apply** (Übernehmen).

Anmelden bei der grafischen Onboard Administrator-Weboberfläche mit der 2-Faktor-Authentifizierung

Navigieren Sie zur grafischen Onboard Administrator-Weboberfläche und klicken Sie auf das entsprechende Benutzerzertifikat, (sofern mehr als eines vorhanden ist). Der Browser sollte zur Bestätigung des Zertifikats auffordern.

Das Zertifikat wird zum Einrichten einer SSL/TLS-Sitzung mit Onboard Administrator benötigt. Wenn die Verbindung erfolgreich hergestellt wurde, werden Sie bei Onboard Administrator als das lokale Benutzerkonto angemeldet, das mit dem Benutzerzertifikat verknüpft ist.

Sollten Probleme auftreten, beziehen Sie sich auf „Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen“ (Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen auf Seite 423).

TFA+LDAP-Authentifizierung

Onboard Administrator unterstützt zusätzlich zur normalen 2-Faktor-Authentifizierung auch die TFA +LDAP-Authentifizierung. In diesem Modus muss der Benutzer:

- über ein auf Onboard Administrator installiertes Benutzerzertifikat verfügen
- die PIN für das Zertifikat kennen
- das zugehörige LDAP-Benutzerkennwort kennen

Die TFA+LDAP-Authentifizierung bietet die folgenden Vorteile:

- Es wird ein größeres Maß an Sicherheit gewährt, da für die Authentifizierung anstelle von zwei drei Punkten entsprochen werden muss.
- Die Autorisierung (Zugriffsberechtigung) wird über LDAP-Gruppen verwaltet, anstatt Benutzerzertifikate einzelnen lokalen Onboard Administrator-Benutzerkonten zuzuordnen.

Wie funktioniert die TFA+LDAP-Authentifizierung

Wenn LDAP konfiguriert ist und das Benutzerzertifikat der 2-Faktor-Authentifizierung keinem lokalen Onboard Administrator-Benutzerkonto zugeordnet ist, dann extrahiert Onboard Administrator bei einem Anmeldeversuch eines Benutzers bei der Onboard Administrator-GUI-Anmeldeseite eine Benutzer-ID aus dem Benutzerzertifikat und fordert den Benutzer zur Eingabe des LDAP-Benutzerkennworts auf.

Der LDAP-Benutzername wird je nach der von Ihnen auf der Registerkarte „Two-Factor Authentification Settings“ (Einstellungen der 2-Faktor-Authentifizierung) vorgenommenen Auswahl entweder aus dem Feld des Antragstellers oder aus dem Feld des alternativen Antragstellernamens des Zertifikats extrahiert und auf der Onboard Administrator-Anmeldeseite angezeigt. Weitere Informationen finden Sie unter „Aktivieren der 2-Faktor-Authentifizierung“ (Aktivieren der 2-Faktor-Authentifizierung auf Seite 420). Bei Auswahl des Antragstellers wird der Benutzername zum Erstellen eines FQDN gemäß RFC 2253 formatiert. Bei Auswahl von **SAN** (Subject Alternative Name, Alternativer Antragstellername) verwendet Onboard Administrator das erste SAN-Feld des Typs EMAIL, OTHERNAME, DNS oder URI im Zertifikat. Die Zertifizierungsstelle steuert die Reihenfolge und den Inhalt der Felder alternativer Antragstellernamen während des Signiervorgangs. Der auf der GUI verwendete Name kann nicht geändert werden.

Nach der Angabe des LDAP-Kennworts finden die folgenden Überprüfungen statt:

- Das Benutzerzertifikat wird anhand der auf Onboard Administrator installierten ZS-Zertifikate überprüft.
- Die LDAP-Anmeldeinformationen werden anhand des konfigurierten LDAP-Servers authentifiziert.
- Der LDAP-Benutzer wird als Mitglied einer autorisierten Gruppe auf dem Onboard Administrator überprüft.

Wenn alle drei Bedingungen erfüllt sind, wird eine Sitzung mit dem Onboard Administrator hergestellt und der Benutzer wird vollständig beim Onboard Administrator angemeldet.

Aktivieren der TFA+LDAP-Authentifizierung

Verfahren Sie zum Verwenden der TFA+LDAP-Authentifizierung wie folgt:

1. Konfigurieren Sie Onboard Administrator gemäß den Anweisungen unter „Konfigurieren des Onboard Administrators für die 2-Faktor-Authentifizierung anhand lokaler Konten“ (Konfigurieren von Onboard Administrator für die 2-Faktor-Authentifizierung anhand lokaler Konten auf Seite 413) für die 2-Faktor-Authentifizierung.
2. Konfigurieren Sie Onboard Administrator zur Verwendung der LDAP-Authentifizierung nach der Beschreibung unter „Bildschirm ‚Directory Settings‘ (Verzeichniseinstellungen)“ (Bildschirm „Directory Settings“ (Verzeichniseinstellungen) auf Seite 328).
3. Melden Sie sich bei Onboard Administrator ausschließlich mittels der 2-Faktor-Authentifizierung an und aktivieren Sie LDAP dann wieder (erforderlich, da LDAP beim Aktivieren der 2-Faktor-Authentifizierung automatisch deaktiviert wird). Weitere Informationen zum Aktivieren von LDAP finden Sie unter „Bildschirm ‚Directory Settings‘ (Verzeichniseinstellungen)“ (Bildschirm „Directory Settings“ (Verzeichniseinstellungen) auf Seite 328) und „Vorbereiten des Verzeichnisses“ (Vorbereiten des Verzeichnisses auf Seite 390).
4. Nachdem überprüft wurde, ob alles erwartungsgemäß funktioniert, können Sie den Zugriff über das lokale Konto durch Deaktivieren des Kontrollkästchens **Enable Local Users** (Lokale Benutzer aktivieren) auf dem Bildschirm „Directory Settings“ (Verzeichniseinstellungen) deaktivieren.

Methoden zur Angabe des Antragstellerfeldes in einer Zertifikatsignieranforderung

Sie können den Inhalt des Feldes **subject** (Antragsteller) in einer Zertifikatsignieranforderung mit beliebigen verschiedenen Methoden steuern:

- Interaktiv in der OpenSSL-Befehlszeile
- Manuell in der OpenSSL-Befehlszeile (ein Beispiel finden Sie unter „Erstellen einer neuen Benutzer-Zertifikatsignieranforderung und eines neuen Serverschlüssels“ (Erstellen einer Benutzer-Zertifikatsignieranforderung und eines neuen Serverschlüssels auf Seite 407))
- In der OpenSSL-Konfigurationsdatei (`.cnf`)
- Über eine komprimierte OpenSSL-Antwortdatei (die Antwortdatei wird von der Zertifizierungsstelle erstellt und enthält Ihren öffentlichen Schlüssel und ist von der Zertifizierungsstelle digital signiert; Sie installieren die Antwortdatei auf dem Webserver)

Verwenden Sie die für Ihre Anforderungen am besten geeignete Methode.

Fehlerbehebung von TFA- und LDAP-Authentifizierungsproblemen

Dieser Abschnitt beschreibt Lösungen für Probleme, die bei der Authentifizierung mit TFA - und LDAP-Zertifikaten möglicherweise auftreten können.

Problem: Browser gibt die Meldung `cannot display webpage` oder `authentication attempt failed` aus.

Lösung: Für das Problem `cannot display webpage`:

1. Stellen Sie sicher, dass die Verwendung des Zertifikats für den SSL-Client genehmigt wurde. Geben Sie beispielsweise den folgenden Befehl aus

   `[ examples]$`**openssl verify -CAfile CA/CA.pem -verbose \-purpose sslclient ./TestUser/certs/test-user.pem**

   `./TestUser/certs/test-user.pem: OK`

2. Stellen Sie sicher, dass dieses Zertifikat dem Browser zur Verfügung steht. (Beziehen Sie sich in Internet Explorer auf **Extras>Internetoptionen>Inhalt>Zertifikate**.)
3. Wenn das Zertifikat auf einem Schlüssel oder in einem Token gespeichert ist, stellen Sie sicher, die Installation ordnungsgemäß vorgenommen wurde.

Wenn die Browser-Meldung `authentication attempt failed` erscheint, war zwar ein Zertifikat mit SSL-Client-Nutzung zum Herstellen der SSL/TLS-Sitzung verfügbar, es lagen aber andere Probleme vor. Versuchen Sie es mit den folgenden Schritten:

1. Stellen Sie mit einem Befehl wie dem Folgenden sicher, dass das Zertifikat gültig ist:

   `[level1CA]$`**openssl verify -CAfile CA/CA.pem -verbose** `-purpose sslclient ~/examples/level1CA/newcerts/0A.pem`

   `..`

   `.`

```
error 9 at 0 depth lookup:certificate is not yet valid
```

2. Wenn das Zertifikat nicht gültig ist, befolgen Sie die Anweisungen in der OpenSSL-Fehlermeldung. Wenn das Zertifikat nicht gültig ist, ist möglicherweise die Systemuhr defekt. Wenn das Zertifikat nicht überprüft werden kann, ist das zugehörige ZS-Zertifikats möglicherweise nicht verfügbar. Gehen Sie zudem folgendermaßen vor:

   a. Stellen Sie sicher, dass die mit dem Zertifikat verknüpften Datumsangaben nicht abgelaufen sind.

   b. Überprüfen Sie die Felder `keyUsage` und `extendedKeyUsage` in der OpenSSL-Konfigurationsdatei der Zertifikatsignieranforderung. Das Feld `keyUsage` gibt die Nutzungseinschränkungen an. Die Nutzung wird durch das Feld `extendedKeyUsage`, sofern vorhanden, noch weiter eingeschränkt.

      Wenn das Feld `extendedKeyUsage` vorhanden ist und nur `clientAuth` angibt, übergibt der Browser (Internet Explorer) das Zertifikat nicht an Onboard Administrator. Dies führt zu der Meldung `cannot display web page`.

      Wenn das Feld `extendedKeyUsage` nicht vorhanden ist, kann das Zertifikat für die Smart Card-Anmeldung verwendet werden. Zum Aktivieren der Zertifikatverwendung in Smart Cards muss das Feld `keyUsage` den Parameter `sslAuth` enthalten. Außerdem muss das Feld `extendedKeyUsage`, sofern vorhanden, die Client-Authentifizierung, Codesignierung und Smart Card-Anmeldung angeben.

      Beispiele:

      Das folgende Zertifikat funktioniert nicht, da die sslClient-Nutzung fehlt:

      ```
      X509v3 Key Usage: critical

              Digital Signature, Non Repudiation
      ```

      Das folgende Zertifikat funktioniert, da alles, was benötigt wird, darin enthalten ist:

      ```
      X509v3 Extended Key Usage:

              TLS Web Client Authentication, E-mail Protection,
      Microsoft Smartcardlogin

            X509v3 Key Usage: critical

              Digital Signature, Non Repudiation, Key Encipherment
      ```

Problem: Probleme bei dem Versuch, zwischen mehreren Client-Benutzern auf demselben System zu wechseln.

Lösung: Manchmal speichern Browser Anmeldeinformationen in einem größeren Umfang als nötig zwischen. Versuchen Sie, das Browsercache zu löschen, wodurch alle temporären Dateien gelöscht werden, und dann alle Browserfenster zu schließen. Andernfalls kann zur Lösung des Problems einfach einen Tag gewartet werden, bis die Sitzungen abgelaufen sind.

Zum Testen mehrerer Clientzertifikate über das gleiche Clientsystem sind möglicherweise separate Anmeldungen erforderlich. Andernfalls kann es vorkommen, dass der Browser das letzte bekannte gültige Zertifikat auswählt.

CLI-Beispiele für das Konfigurieren eines Benutzerkontos und von Zertifikaten

Das folgende Beispiel zeigt Onboard Administrator-CLI-Befehle, die zum Konfigurieren eines lokalen Benutzerkontos und von Zertifikaten verwendet werden. Das Beispiel wird anschließend kommentiert.

```
=======================================

== Add user, CA certs, and user cert

=======================================

set script mode on

add user "marc" "password"

set user contact "marc" "800-555-1212"

set user fullname "marc" "Marc Last-name"

set user access "marc" ADMINISTRATOR

enable user "marc"

assign server all "marc"

assign interconnect all "marc"

assign oa "marc"

show user "marc"

download ca certificate http://dev-srvr/certs/Common-Policy.cer

download ca certificate http://dev-srvr/certs/SHA-1-Federal-Root-CA.cer

download ca certificate http://dev-srvr/certs/DoD-Interoperability-Root-
CA-1.cer

download ca certificate http://dev-srvr/certs/DoD-Root-CA-2.cer

download ca certificate http://dev-srvr/certs/DOD-EMAIL-CA-19.cer

download user certificate "marc" http://dev-srvr/certs/Marc-Lastname.cer

show user "marc"

set script mode off

================================================

== Go to the GUI, enable TFA, then

== log in via the Web browser using the TFA token.

================================================

=======================================

== Remove Fed certificates and user

=======================================

set script mode on
```

```
remove ca certificate "CD:78:54:4C:CA:C6:EA:15:72:81:86:EB:
86:59:F6:E6:C0:FA:A7:41"

remove ca certificate "B1:10:5C:D1:0F:C3:70:F5:6B:89:DD:1D:49:F6:D8:30:DF:
35:F2:DE"

remove ca certificate "FD:F3:F4:F8:C7:3B:5A:
63:20:62:08:88:29:00:D1:92:B1:75:BA:E8"

remove ca certificate "30:BE:4D:
40:F6:10:E5:65:B3:53:F3:44:C7:27:64:1E:EE:E7:86:D2"

remove ca certificate "CB:44:A0:97:85:7C:45:FA:18:7E:D9:52:08:6C:B9:84:1F:
2D:51:B5"

remove user certificate "Marc"

remove user "marc"

set script mode off
```

Die Befehle im ersten Abschnitt des Beispiels fügen einen Benutzer mit Administrator-Berechtigungen hinzu und installieren Zertifikate:

- Fügt ein Benutzerkonto hinzu (`ADD USER`)
- Legt Benutzereigenschaften fest (`SET USER`)
- Aktiviert ein Benutzerkonto (`ENABLE USER`)
- Weist alle Server und Verbindungsmoduleinschübe der Steuerung durch den Benutzer zu (`ASSIGN SERVER ALL`, `ASSIGN INTERCONNECT ALL`)
- Gewährt den Onboard Administrator-Einschüben die angegebene Benutzerzugriffsberechtigung (`ASSIGN OA`)
- Zeigt Benutzerinformationen, die Benutzerzugriffsebene und die dem Benutzer zugewiesenen Einschübe an (`SHOW USER`)
- Installiert ZS-Zertifikate von den angegebenen Speicherorten (`DOWNLOAD CA CERTIFICATE`)
- Installiert ein Benutzerzertifikat von dem angegebenen Speicherort (`DOWNLOAD USER CERTIFICATE`)

Die Skript-Kommentare erinnern daran, die 2-Faktor-Authentifizierung über die Onboard Administrator-GUI zu aktivieren und sich dann mittels des entsprechenden TFA-Schlüssels über den Webbrowser anzumelden.

Der zweite Abschnitt des Beispiels:

- Entfernt ZS-Zertifikate (`REMOVE CA CERTIFICATE`)
- Entfernt ein Benutzerzertifikat (`REMOVE USER CERTIFICATE`)
- Entfernt einen Benutzer (`REMOVE USER`)

Über das Internet verfügbare Informationen zu Zertifizierungsstellen und Zertifikaten

Weitere Informationen zum Verwalten von Zertifizierungsstellen und Zertifikaten finden Sie auf den folgenden Websites:

- Website der OpenSSL-Dokumentation (http://www.openssl.org/docs)
- Website des Linux-Dokumentationsprojekts (http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO) (Wie Zertifizierungsstellen verwaltet und SSL-Zertifikate ausgeben oder signiert werden)
- G-Loaded Journal-Website (http://www.g-loaded.eu/2005/11/10/be-your-own-ca/) (Wie Zertifizierungsstellen erstellt und Serverzertifikate ausgegeben werden)
- Debian Administration-Website (http://www.debian-administration.org/articles/284) (Erstellen und Verwenden selbstsignierter Zertifikate)

14 Zeitzoneneinstellungen

Zeitzoneneinstellungen für die Universalzeit

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für die Universalzeit, die von Onboard Administrator unterstützt werden.

CET	Etc/GMT+2	Etc/GMT+8	Etc/UCT	MST
CST6CDT	Etc/GMT-3	Etc/GMT-9	Etc/Universal	MST7MDT
EET	Etc/GMT+3	Etc/GMT+9	Etc/UTC	Navajo
EST	Etc/GMT-4	Etc/GMT-10	Etc/Zulu	PST8PDT
EST5EDT	Etc/GMT+4	Etc/GMT+10	Werkseinstellung	UCT
Etc/GMT	Etc/GMT-5	Etc/GMT-11	GMT	Universal
Etc/GMT0	Etc/GMT+5	Etc/GMT+11	GMT+0	UTC
Etc/GMT-0	Etc/GMT-6	Etc/GMT-12	GMT0	WET
Etc/GMT+0	Etc/GMT+6	Etc/GMT+12	GMT-0	W-SU
Etc/GMT-1	Etc/GMT-7	Etc/GMT-13	Greenwich	Zulu
Etc/GMT+1	Etc/GMT+7	Etc/GMT-14	HST	—
Etc/GMT-2	Etc/GMT-8	Etc/Greenwich	MET	—

Zeitzoneneinstellungen für Afrika

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für Afrika, die von Onboard Administrator unterstützt werden.

Africa/Abidjan	Africa/Ceuta	Africa/Kinshasa	Africa/Niamey
Africa/Accra	Africa/Conakry	Africa/Lagos	Africa/Nouakchott
Africa/Addis_Ababa	Africa/Dakar	Africa/Libreville	Africa/Ouagadougou
Africa/Algiers	Africa/Dar_es_Salaam	Africa/Lome	Africa/Porto-Novo
Africa/Asmara	Africa/Djibouti	Africa/Luanda	Africa/Sao_Tome
Africa/Asmera	Africa/Douala	Africa/Lubumbashi	Africa/Timbuktu
Africa/Bamako	Africa/El_Aaiun	Africa/Lusaka	Africa/Tripoli
Africa/Bangui	Africa/Freetown	Africa/Malabo	Africa/Tunis

Africa/Banjul	Africa/Gaborone	Africa/Maputo	Africa/Wjndhoek
Africa/Bissau	Africa/Harare	Africa/Maseru	Egypt
Africa/Blantyre	Africa/Johannesburg	Africa/Mbabane	Libya
Africa/Brazzaville	Africa/Juba	Africa/Mogadishu	—
Africa/Bujumbura	Africa/Kampala	Africa/Monrovia	—
Africa/Cairo	Africa/Khartoum	Africa/Nairobi	—
Africa/Casablanca	Africa/Kigali	Africa/Ndjamena	—

Zeitzoneneinstellungen für Amerika

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für Amerika, die von Onboard Administrator unterstützt werden.

America/Adak	America/Guatemala	America/Rainy_River
America/Anchorage	America/Guayaquil	America/Rankin_Inlet
America/Anguilla	America/Guyana	America/Recife
America/Antigua	America/Halifax	America/Regina
America/Araguaina	America/Havana	America/Resolute
America/Argentina/Buenos_Aires	America/Hermosillo	America/Rio_Branco
America/Argentina/Catamarca	America/Indiana/Indianapolis	America/Rosario
America/Argentina/ComodRivadavia	America/Indiana/Knox	America/Santa_Isabel
America/Argentina/Cordoba	America/Indiana/Marengo	America/Santarem
America/Argentina/Jujuy	America/Indiana/Petersburg	America/Santiago
America/Argentina/La_Rioja	America/Indiana/Tell_City	America/Santo_Domingo
America/Argentina/Mendoza	America/Indiana/Vevay	America/Sao_Paulo
America/Argentina/Rio_Gallegos	America/Indiana/Vincennes	America/Scoresbysund
America/Argentina/Salta	America/Indiana/Winamac	America/Shiprock
America/Argentina/San_Juan	America/Indianapolis	America/Sitka
America/Argentina/San_Luis	America/Inuvik	America/St_Barthelemy
America/Argentina/Tucuman	America/Iqaluit	America/St_Johns
America/Argentina/Ushuaia	America/Jamaica	America/St_Kitts
America/Aruba	America/Jujuy	America/St_Lucia
America/Asuncion	America/Juneau	America/St_Thomas
America/Atikokan	America/Kentucky/Louisville	America/St_Vincent
America/Atka	America/Kentucky/Monticello	America/Swift_Current

America/Bahia	America/Knox_IN	America/Tegucigalpa
America/Bahia_Banderas	America/Kralendijk	America/Thule
America/Barbados	America/La_Paz	America/Thunder_Bay
America/Belem	America/Lima	America/Tijuana
America/Belize	America/Los_Angeles	America/Toronto
America/Blanc-Sablon	America/Louisville	America/Tortola
America/Boa_Vista	America/Lower_Princes	America/Vancouver
America/Bogota	America/Maceio	America/Virgin
America/Boise	America/Managua	America/Whitehorse
America/Buenos_Aires	America/Manaus	America/Winnipeg
America/Cambridge_Bay	America/Marigot	America/Yakutat
America/Campo_Grande	America/Martinique	America/Yellowknife
America/Cancun	America/Matamoros	Brazil/Acre
America/Caracas	America/Mazatlan	Brazil/DeNoronha
America/Catamarca	America/Mendoza	Brazil/East
America/Cayenne	America/Menominee	Brazil/West
America/Cayman	America/Merida	Canada/Atlantic
America/Chicago	America/Metlakatla	Canada/Central
America/Chihuahua	America/Mexico_City	Canada/Eastern
America/Coral_Harbour	America/Miquelon	Canada/East-Saskatchewan
America/Cordoba	America/Moncton	Canada/Mountain
America/Costa_Rica	America/Monterrey	Canada/Newfoundland
America/Creston	America/Montevideo	Canada/Pacific
America/Cuiaba	America/Montreal	Canada/Saskatchewan
America/Curacao	America/Montserrat	Canada/Yukon
America/Danmarkshavn	America/Nassau	Chile/Continental
America/Dawson	America/New_York	Chile/EasterIsland
America/Dawson_Creek	America/Nipigon	Cuba
America/Denver	America/Nome	Jamaica
America/Detroit	America/Noronha	Mexico/BajaNorte
America/Dominica	America/North_Dakota/Beulah	Mexico/BajaSur
America/Edmonton	America/North_Dakota/Center	Mexico/General
America/Eirunepe	America/North_Dakota/New_Salem	US/Alaska
America/El_Salvador	America/Ojinaga	US/Aleutian
America/Ensenada	America/Panama	US/Arizona

America/Fort_Wayne	America/Pangnirtung	US/Central
America/Fortaleza	America/Paramaribo	US/Eastern
America/Glace_Bay	America/Phoenix	US/East-Indiana
America/Godthab	America/Port_of_Spain	US/Indiana-Starke
America/Goose_Bay	America/Port-au-Prince	US/Michigan
America/Grand_Turk	America/Porto_Acre	US/Mountain
America/Grenada	America/Porto_Velho	US/Pacific
America/Guadeloupe	America/Puerto_Rico	US/Pacific-New

Zeitzoneneinstellungen für Asien

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für Asien, die von Onboard Administrator unterstützt werden.

Asia/Aden	Asia/Dhaka	Asia/Khandyga	Asia/Qyzylorda	Asia/Ulaanbaatar
Asia/Almaty	Asia/Dili	Asia/Kolkata	Asia/Rangoon	Asia/Ulan_Bator
Asia/Amman	Asia/Dubai	Asia/Krasnoyarsk	Asia/Riyadh	Asia/Urumqi
Asia/Anadyr	Asia/Dushanbe	Asia/Kuala_Lumpur	Asia/Riyadh87	Asia/Ust-Nera
Asia/Aqtau	Asia/Gaza	Asia/Kuching	Asia/Riyadh88	Asia/Vientiane
Asia/Aqtobe	Asia/Harbin	Asia/Kuwait	Asia/Riyadh89	Asia/Vladivostok
Asia/Ashgabat	Asia/Hebron	Asia/Macao	Asia/Saigon	Asia/Yakutsk
Asia/Ashkhabad	Asia/Ho_Chi_Minh	Asia/Macau	Asia/Sakhalin	Asia/Yekaterinburg
Asia/Baghdad	Asia/Hong_Kong	Asia/Magadan	Asia/Samarkand	Asia/Yerevan
Asia/Bahrain	Asia/Hovd	Asia/Makassar	Asia/Seoul	Hongkong
Asia/Baku	Asia/Irkutsk	Asia/Manila	Asia/Shanghai	Iran
Asia/Bangkok	Asia/Istanbul	Asia/Muscat	Asia/Singapore	Israel
Asia/Beirut	Asia/Jakarta	Asia/Nicosia	Asia/Taipei	Japan
Asia/Bishkek	Asia/Jayapura	Asia/Novokuznetsk	Asia/Tashkent	Mideast/Riyadh87
Asia/Brunei	Asia/Jerusalem	Asia/Novosibirsk	Asia/Tbilisi	Mideast/Riyadh88
Asia/Choibalsan	Asia/Kabul	Asia/Omsk	Asia/Tehran	Mideast/Riyadh89
Asia/Chongqing	Asia/Kamchatka	Asia/Oral	Asia/Tel_Aviv	PRC
Asia/Chungking	Asia/Karachi	Asia/Phnom_Penh	Asia/Thimbu	ROC
Asia/Colombo	Asia/Kashgar	Asia/Pontianak	Asia/Thimphu	ROK

Asia/Dacca	Asia/Kathmandu	Asia/Pyongyang	Asia/Tokyo	Singapore
Asia/Damascus	Asia/Katmandu	Asia/Qatar	Asia/Ujung_Pandang	Turkey

Zeitzoneneinstellungen für Ozeanien

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für Ozeanien, die von Onboard Administrator unterstützt werden.

Atlantic/Azores	Australia/Melbourne	Kwajalein	Pacific/Marquesas
Atlantic/Bermuda	Australia/North	NZ	Pacific/Midway
Atlantic/Canary	Australia/NSW	NZ-CHAT	Pacific/Nauru
Atlantic/Cape_Verde	Australia/Perth	Pacific/Apia	Pacific/Niue
Atlantic/Faeroe	Australia/Queensland	Pacific/Auckland	Pacific/Norfolk
Atlantic/Jan_Mayen	Australia/South	Pacific/Chatham	Pacific/Noumea
Atlantic/Madeira	Australia/Sydney	Pacific/Chuuk	Pacific/Pago_Pago
Atlantic/Reykjavik	Australia/Tasmania	Pacific/Easter	Pacific/Palau
Atlantic/South_Georgia	Australia/Victoria	Pacific/Efate	Pacific/Pitcairn
Atlantic/St_Helena	Australia/West	Pacific/Enderbury	Pacific/Pohnpei
Atlantic/Stanley	Australia/Yancowinna	Pacific/Fakaofo	Pacific/Ponape
Australia/ACT	Iceland	Pacific/Fiji	Pacific/Port_Moresby
Australia/Adelaide	Indian/Antananarivo	Pacific/Funafuti	Pacific/Rarotonga
Australia/Brisbane	Indian/Chagos	Pacific/Galapagos	Pacific/Saipan
Australia/Broken_Hill	Indian/Christmas	Pacific/Gambier	Pacific/Samoa
Australia/Canberra	Indian/Cocos	Pacific/Guadalcanal	Pacific/Tahiti
Australia/Currie	Indian/Comoro	Pacific/Guam	Pacific/Tarawa
Australia/Darwin	Indian/Kerguelen	Pacific/Honolulu	Pacific/Tongatapu
Australia/Eucla	Indian/Mahe	Pacific/Johnston	Pacific/Truk
Australia/Hobart	Indian/Maldives	Pacific/Kiritimati	Pacific/Wake
Australia/LHI	Indian/Mauritius	Pacific/Kosrae	Pacific/Wallis
Australia/Lindeman	Indian/Mayotte	Pacific/Kwajalein	Pacific/Yap
Australia/Lord_Howe	Indian/Reunion	Pacific/Majuro	US/Hawaii
—	—	—	US/Samoa

Zeitzoneneinstellungen für Europa

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für Europa, die von Onboard Administrator unterstützt werden.

Eire	Europe/Kaliningrad	Europe/Sarajevo
Europe/Amsterdam	Europe/Kiev	Europe/Simferopol
Europe/Andorra	Europe/Lisbon	Europe/Skopje
Europe/Athens	Europe/Ljubljana	Europe/Sofia
Europe/Belfast	Europe/London	Europe/Stockholm
Europe/Belgrade	Europe/Luxembourg	Europe/Tallinn
Europe/Berlin	Europe/Madrid	Europe/Tirane
Europe/Bratislava	Europe/Malta	Europe/Tiraspol
Europe/Brussels	Europe/Mariehamn	Europe/Uzhgorod
Europe/Bucharest	Europe/Minsk	Europe/Vaduz
Europe/Budapest	Europe/Monaco	Europe/Vatican
Europe/Busingen	Europe/Moscow	Europe/Vienna
Europe/Chisinau	Europe/Nicosia	Europe/Vilnius
Europe/Copenhagen	Europe/Oslo	Europe/Volgograd
Europe/Dublin	Europe/Paris	Europe/Warsaw
Europe/Gibraltar	Europe/Podgorica	Europe/Zagreb
Europe/Guernsey	Europe/Prague	Europe/Zaporozhye
Europe/Helsinki	Europe/Riga	Europe/Zurich
Europe/Isle_of_Man	Europe/Rome	GB
Europe/Istanbul	Europe/Samara	GB-Eire
Europe/Jersey	Europe/San_Marino	Poland
—	—	Portugal

Zeitzoneneinstellungen für Polar-Zeit

HINWEIS: Die Zeitzonen müssen exakt so eingegeben werden, wie unten in der Tabelle angegeben.

Die folgende Tabelle enthält die Zeitzoneneinstellungen für die Polar-Zeit, die von Onboard Administrator unterstützt werden.

Antarctica/Casey	Antarctica/Mawson	Antarctica/South_Pole

Antarctica/Davis	Antarctica/McMurdo	Antarctica/Syowa
Antarctica/DumontDUrville	Antarctica/Palmer	Antarctica/Vostok
Antarctica/Macquarie	Antarctica/Rothera	Arctic/Longyearbyen

15 Support und andere Ressourcen

Vor der Kontaktaufnahme mit HP

Bitte halten Sie die nachfolgend aufgeführten Informationen bereit, wenn Sie bei HP anrufen:

- Active Health System-Protokoll (HP ProLiant Gen8 oder spätere Produkte)

  Laden Sie ein Active Health System-Protokoll herunter, das die sieben (7) Tage vor dem Auftreten der Störung umfasst, und halten Sie es bereit. Weitere Informationen enthält das *HP iLO 4 Benutzerhandbuch* oder das *HP Intelligent Provisioning Benutzerhandbuch* auf der HP Website (http://www.hp.com/go/ilo/docs).

- Onboard Administrator SHOW ALL-Bericht (nur für HP BladeSystem Produkte)

  Weitere Informationen zum Anfordern des Onboard Administrator SHOW ALL-Berichts finden Sie auf der HP-Website (http://www.hp.com/go/OAlog).

- Registrierungsnummer beim Technischen Support (sofern zutreffend)
- Seriennummer des Produkts
- Modellname und -nummer des Produkts
- Produkt-Identifizierungsnummer
- Eventuell vorliegende Fehlermeldungen
- Zusätzlich installierte Platinen oder Hardware
- Software und Hardware von Fremdherstellern
- Betriebssystem und Revisionsstufe

HP Kontaktinformationen

Kontaktinformationen für die USA und weltweite Kontaktinformationen finden Sie auf der Website „Contact HP“ (Kontaktaufnahme mit HP) (http://www.hp.com/go/assistance).

In den USA:

- Telefonisch können Sie HP unter der Nummer +1-800-334-5144 erreichen. Zwecks kontinuierlicher Qualitätsverbesserung können die Aufrufe aufgezeichnet oder überwacht werden.
- Wenn Sie ein Care Pack (Service-Upgrade) erworben haben, informieren Sie sich auf der Website für Support und Treiber (http://www8.hp.com/us/en/support-drivers.html). Wenn sich das Problem nicht über die Website lösen lässt, rufen Sie die Nummer +1-800-633-3600 an. Weitere Informationen zu Care Packs finden Sie auf der HP Website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html)

Weitere Informationen

Für Folgendes ...	Beziehen Sie sich auf ...
HP Onboard Administrator-Dokumentation, einschließlich der Benutzerhandbücher und Versionshinweise	HP Onboard Administrator-Informationsbibliothek (http://www.hp.com/support/oa/docs)
HP BladeSystem c3000/c7000-Gehäuse-Dokumentation	HP BladeSystem-Informationsbibliothek (http://www.hp.com/support/BladeSystem/docs)
HP Scripting Tools für Windows PowerShell OA cmdlets	HP Scripting Tools für PowerShell Library (http://www.hp.com/go/powershell/docs)
HP Onboard Administrator-Produktinformationen und zusätzliche Ressourcen, einschließlich Links zu QuickSpecs, Benutzerhandbüchern, Versionshinweisen, Whitepapers und anderer Dokumentation	HP Onboard Administrator-Produkt-Website (http://www.hp.com/go/oa)
HP Insight Management-Dokumentation	HP Insight Management-Informationsbibliothek (http://www.hp.com/go/insightmanagement/docs)
iLO Management Engine-Dokumentation	HP iLO Management Engine-Informationsbibliothek (http://www.hp.com/go/ilomgmtengine/docs)
HP Insight Remote Support-Dokumentation	HP Insight Remote Support Informationsbibliothek (http://www.hp.com/go/insightremotesupport/docs)

16 Akronyme und Abkürzungen

CA

Certificate Authority (Zertifizierungsstelle)

CRL

Certification Revocation List (Zertifikatsperrliste)

CSR

Certificate Signing Request (Zertifikatsignieranforderung)

DC

Domain Controller (Domänencontroller)

DCC

Device Control Channel (Gerätesteuerkanal)

DHCP

Dynamic Host Configuration Protocol

DN

Distinguished Name (Definierter Name)

DNS

Domain Name System

EBIPA

Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub)

EDPC

Enclosure Dynamic Power Capping (Gehäusedynamische Stromobergrenzen)

EEPROM

Electrical Erasable Programmable Read Only Memory

EFM

Enclosure Firmware Management

FIPS

Federal Information Processing Standard

FQDN

Fully Qualified Domain Name (Vollqualifizierter Domänenname)

FRU

Field Replaceable Unit (Vor Ort austauschbare Einheit)

GC

Global Catalog (Globaler Katalog)

HPSC

HP Support Center

HTTPS

Hypertext Transfer Protocol Secure Sockets

I2C

Inter-integrated Circuit (Inter-integrierter Schaltkreis)

iLO

Integrated Lights-Out

KVM

Keyboard, Video, Mouse (Tastatur, Monitor, Maus)

LDAP

Lightweight Directory Access Protocol

LOM

LAN on Motherboard (LAN auf Hauptplatine)

MAC

Media Access Control

MMC

Microsoft Management Console

NTP

Network Time Protocol

NVRAM

Nonvolatile Memory (Nichtflüchtiger Speicher)

PCI

Payment Card Industry

PCIe

Peripheral Component Interconnect Express

PEM

Privacy Enhanced Mail

PIC

Peripheral Interface Controller

PIN

Personal Identification Number

PKCS

Public-Key Cryptography Standards

PXE

Preboot Execution Environment

RBSU

ROM-Based Setup Utility (ROM-basiertes Setup-Programm)

RIBCL

Remote Insight Board Command Language (Befehlssprache für das Remote Insight Board)

RPM

Red Hat Package Manager

RSA

Verschlüsselungsverfahren nach Rivest, Shamir und Adelman, das auf dem Prinzip des öffentlichen Schlüssels beruht

SAM

Security Account Manager

SAS

Serial Attached SCSI (Seriell verbundener SCSI)

SLAAC

Stateless Address Auto Configuration (Statuslose automatische Konfiguration von Adressen)

SOAP

Simple Object Access Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

SUV

Serial, USB, Video (Seriell, USB, Monitor)

TFA

Two-Factor Authentication (2-Faktor-Authentifizierung)

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security

TPM

Trusted Platform Module

UEFI

Unified Extensible Firmware Interface

UID

Unit Identification (Geräteidentifizierung)

VC

Virtual Connect

VCM

Virtual Connect Manager

VLAN

Virtual Local-Area Network (Virtuelles lokales Netzwerk)

VSP

Virtual Serial Port

17 Feedback zur Dokumentation

HP hat sich zur Bereitstellung von Dokumentation verpflichtet, die Ihre Anforderungen erfüllt. Um uns in unseren Bemühungen zu unterstützen, die Dokumentation ständig zu verbessern, senden Sie bitte Fehler, Vorschläge oder Kommentare an Documentation Feedback (mailto:docsfeedback@hp.com). Geben Sie dabei den Dokumenttitel, die Teilenummer, die Versionsnummer oder die URL an.

Index

Symbole/Zahlen

2-Faktor-Authentifizierung
  2-Faktor-Authentifizierung 344
  Erstellen von Zertifizierungsstellen und Konfigurieren der 2-Faktor-Authentifizierung für lokale Benutzer- und LDAP-Gruppenkonten 398
2-Faktor-Authentifizierung, Erstellen einer Stammzertifizierungsstelle 402
  Erstellen untergeordneter Zertifizierungsstellen 404
  Installieren der Zertifizierungsstellenkette für TFA 415
2-Faktor-Authentifizierung, Aktivieren
  Aktivieren der 2-Faktor-Authentifizierung 420
  Two-Factor Authentication (2-Faktor-Authentifizierung) 344
2-Faktor-Authentifizierung, Anmelden bei der OA-GUI 421
2-Faktor-Authentifizierung, Benutzerzertifikate
  2-Faktor-Authentifizierung 344
  Bereitstellen von x 509-Benutzerzertifikatinformationen 407
  Installieren von Benutzerzertifikaten auf dem lokalen Administratorkonto 418
  Registerkarte „Edit Local User Certificate Information“ (Zertifikatinformationen des lokalen Benutzers bearbeiten) 327
  Registerkarte „Two-Factor Authentication Certificate Information“ (Zertifikatinformationen der 2-Faktor-Authentifizierung) 345
  Registerkarte „Two-Factor Authentication Certificate Upload“ (Hochladen des Zertifikats der 2-Faktor-Authentifizierung) 346
  Signieren der Benutzer-Zertifikatsignieranforderung mit dem level1CA-Schlüssel 408
  Speichern eines Benutzerzertifikats auf einer Smart Card oder einem Browser 411
  Überprüfen von Zertifikaten 410
2-Faktor-Authentifizierung, CLI-Konfigurationsbeispiele 425
2-Faktor-Authentifizierung, Erstellen eines Benutzerschlüssels 406
2-Faktor-Authentifizierung, Infrastruktur öffentlicher Schlüssel 398
2-Faktor-Authentifizierung, Konfigurieren anhand von lokalen Benutzerkonten 413
2-Faktor-Authentifizierung, Konfigurieren anhand von lokalen Benutzer- und LDAP-Gruppenkonten 398
2-Faktor-Authentifizierung, Konfigurieren der Verzeichnisse für Zertifikate 400
2-Faktor-Authentifizierung, plus LDAP 421
2-Faktor-Authentifizierung, Serverzertifikate 404
2-Faktor-Authentifizierung, Sitzungszeitlimit 414
2-Faktor-Authentifizierung, Speichern von Zertifikaten 411
2-Faktor-Authentifizierung, Überprüfen von Zertifikaten
  Überprüfen von Zertifikaten 410
  Verschiedene bekannte Probleme 387
2-Faktor-Authentifizierung, Übersicht 398
2-Faktor-Authentifizierung, weitere Informationen zu Zertifizierungsstellen und Zertifikaten 426
2-Faktor-Authentifizierung, Wiederherstellungsplan 413
2-Faktor-Authentifizierung mit LDAP, Fehlerbehebung 423

A

Active Health System 184
Active to Standby (Aktiv in Standby) 161
Afrika, Zeitzone 428
Aktivieren von IPv6 129
Amerika, Zeitzone 429
Ändern von Einstellungen, Gehäuse 14
Anforderungen, Onboard Administrator 3
Anforderungen, Zugriff 3
Angemeldete Benutzer 346
Anmelde-Banner
  Network Access (Netzwerkzugriff) 136
  Registerkarte „Login Banner“ (Anmelde-Banner) 142
Anmelden bei Onboard Administrator 10
Anschluss, seriell 352
Ansicht des Racks
  Ansicht des Racks 100
  Bildschirm „Rack Overview“ (Rack-Übersicht) 100
Anzeigesprache 56

Asien, Zeitzone 431
Ausschalten 207
Authentifizieren von Benutzern 7

B
Befehlszeilenschnittstelle, verwenden 350
Befehlszeilenschnittstelle (Command Line Interface, CLI) 350
Bekannte Probleme
  Bekannte Browser-Probleme 385
  Bekannte Netzwerkprobleme 387
  Verschiedene bekannte Probleme 387
Benutzer, angemeldete 346
Benutzerauthentifizierungsmenü 320
Benutzereinstellungen 56, 323
Benutzerkonten 7
Benutzerkonto, ändern 65
Benutzerkonto, hinzufügen
  Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
  Lokale Benutzer 322
Benutzerkonto, löschen
  Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
  Lokale Benutzer 322
Benutzernotiz, Bildschirm 44
Benutzerrollen 7
Benutzerverwaltung 320
Berechtigungsebenen
  Bearbeiten einer LDAP-Gruppe 339
  Edit Local User (Lokalen Benutzer bearbeiten) 323
  Hinzufügen einer LDAP-Gruppe 337
Betriebssystem-Bereitstellung, unbeaufsichtigte 170
Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator) 208
Bildschirm „Blade or Port Info“ (Blade- oder Port-Info) 40
Bildschirm „Chat Mode“ (Chat-Modus) 44
Bildschirm „Enclosure Info“ (Gehäuse-Info) 41
Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) 40
Bildschirm „KVM Menu“ (KVM-Menü) 46
Bildschirm „Power and Thermal“ (Stromversorgung und Wärmewerte) 295
Bildschirm „SNMP Settings“ (TCP/IP-Einstellungen) 143
Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator 212
Bildschirm „USB Key Menu“ (USB-Schlüssel-Menü) 45
BladeSystem-Netzwerkarchitektur 16
Browser, Fehlerbehebung 385
Browseranforderungen
  Bekannte Browser-Probleme 385
  Zugriffsanforderungen 3

C
CA (Zertifizierungsstelle) 390
CD-ROM-Laufwerk
  DVD-Laufwerk 162
  Interaktive Installation und Konfiguration des DVD/CD-ROM-Laufwerks 164
Chiffren
  Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
  Registerkarte „FIPS“ 140
CLI, Zugriff abgelehnt 387
CLI (Befehlszeilenschnittstelle) 350
CSR-Erstellungsfehler 387
Current Default Gateway (Aktuelles Standard-Gateway)
  Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator 212
  Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA 230

D
Datum und Uhrzeit 123
DHCPv6 Address (IP-Adresse) 212
Diagnoseprobleme 360
DNS-Server 230
Dokumentation
  Weitere Informationen 436
DVD-Laufwerk
  DVD-Laufwerk 162
  Interaktive Installation und Konfiguration des DVD/CD-ROM-Laufwerks 164
  Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade) 248
DVD-Verbindung
  Geräteeinschübe 237
  Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade) 248
Dynamic DNS (Dynamisches DNS)
  Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
  Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
  Registerkarte „IPv4-Einstellungen“ 126
  Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
  Registerkarte „NIC Options“ (NIC-Optionen) 135
Dynamic Host Configuration Protocol (DHCP)
  Bildschirm „Onboard Administrator Network

Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator 212
Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) 126
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA 230
Dynamic Power (Dynamischer Stromsparmodus)
Bildschirm „Power Management“ (Stromversorgungsverwaltung) 88
Durchführen der Insight Display-Installation 31
Power Management 296
Dynamische Obergrenze des Gehäuses 295

E
EBIPA, Einstellungen 66
EBIPA, Servereinschub 66
EBIPA (Enclosure Bay IP Addressing, IP-Adressierung für Komponenteneinschübe). 148
EBIPA für IPv4 151
EBIPA für IPv6 154
EBIPA-Konfigurationsrichtlinien
Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub) 66, 148
Edit VLAN (VLAN bearbeiten) 180
Einrichten des Administratorkontos 64
Einstellungen, Gehäuse
Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
Gehäuseeinstellungen 111
Einstellungen, Kennwort 327
Einstellungen, NIC 230
Einstellungen des Sitzungszeitlimits
Konfigurieren des Onboard Administrator-Sitzungszeitlimits 414
Einstellungen für E-Mail-Benachrichtigung 116
Einstellungen für Sitzungszeitlimit (Timeout)
Registerkarte „Session Options“ (Sitzungsoptionen) 347
E-Mail-Benachrichtigung 116
Enclosure Firmware Management
Enclosure Firmware Management 197
Firmware 270
Enclosure Firmware Management-Protokoll
Enclosure Firmware Management-Protokoll 205
Firmware-Management-Protokolle 275
Ereignisprotokolle
Insight Remote Support-Datensammlungen 193
Insight Remote Support-Serviceereignisse 192
Erweiterte Sicherheitseinstellungen 140
Erweitertes Systemprotokoll 226
Erzwingen einer starken Verschlüsselung
FIPS 57
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Network Access (Netzwerkzugriff) 136
Registerkarte „FIPS“ 140
Europa, Zeitzone 433

F
Failover 143
Failover, erzwingen 161
Failover bei Verbindungsverlust 143
Fehler, Installation 48
Fehler, Komponentenausfall 48
Fehler, Konfiguration 48
Fehler, Kühlung 47
Fehler, Lüfter 47
Fehler, Position 48
Fehler, Stromversorgung 47
Fehlerbeseitigung 360
Fehlerbeseitigung, Firmwareaktualisierungs-programm 360
Fehlerdiagnose 360
Fehlermeldungen 360
Fehlermeldungen, Insight Display 47
Fehlgeschlagene Ereignisse 205
FIPS-Modus, Aktivieren
FIPS 57
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140
FIPS-Modus, Standardeinstellungen 18
Firmware, Herabstufung 222
Firmwareaktualisierung 222
Firmwareaktualisierungs-programm, Fehlerbeseitigung 360
Firmware-Übersicht 106
Firmwareversion, anzeigen
Anzeigen der Firmware-Versionen 277
Bildschirm „Rack Firmware“ (Rack-Firmware) 106
Enclosure Firmware Management 197
Firmwareversionen, abweichende 279
Flash-Notfallwiederherstellung 12
FQDN-Link-Unterstützung
Bildschirm „Interconnect Bay Summary“ (Zusammenfassung der Verbindungsmoduleinschübe) 286
Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub) 288
Bildschirm „Rack Overview“ (Rack-Übersicht) 100
Geräteeinschübe 237

iLO-Bildschirm 253
Virtual Connect Manager 348

G
Gateway-Adresse
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
EBIPA für IPv4 151
EBIPA für IPv6 154
Enclosure Bay IP Addressing (IP-Adressierung für den Gehäuseeinschub) 66
Registerkarte „IPv4-Einstellungen“ 126
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA 230
Gehäuse, ausschalten 207
Gehäuse, auswählen
Auswählen von Gehäusen 111
Bildschirm „Enclosure Selection“ (Gehäuseauswahl) 59
Gehäuse, Einstellungen
Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
Bildschirm „Rack and Enclosure Settings“ (Rack- und Gehäuseeinstellungen) 61
Gehäuseeinstellungen 111
Gehäuse, konfigurieren 110
Gehäuse, verbinden 207
Gehäuse, verwalten
Übersicht über Onboard Administrator 4
Verwalten von Gehäusen 207
Gehäuse, virtuelle Tasten 111
Gehäuseeinstellungen 111
Gehäuse-KVM-Funktionen 50
Gehäusestatusinformationen
Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator 10
Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
Gehäuse-UID, umschalten 111
Geräteeinschub, Status-Registerkarte
Registerkarte „Device Bay Status“ (Status des Geräteeinschubs) 240
Registerkarte „Server Blade Information“ (Server Blade-Informationen) 245
Geräteeinschub, Übersichtsbildschirm 237
Geräteeinschübe
Geräteeinschübe 237
Geräteeinschübe, Startsequenz 120
Grafische Ansicht 357

H
Herunterladen von Dateien 435
Hinzufügen einer Verzeichnisgruppe
Erstellen von Verzeichnisgruppen 394
Hinzufügen einer LDAP-Gruppe 337
Hinzufügen eines Benutzers
Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
Lokale Benutzer 322
Hinzufügen von VLAN 180
HP BladeSystem Insight Display 28
HP BladeSystem Insight Display, Bildschirm „Blade or Port Info“ (Blade- oder Port-Info) 41
HP BladeSystem Insight Display, Bildschirm „Chat Mode“ (Chat-Modus) 44
HP BladeSystem Insight Display, Bildschirm „Enclosure Info“ (Gehäuse-Info) 41
HP BladeSystem Insight Display, Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) 40
HP BladeSystem Insight Display, Bildschirm „KVM Menu“ (KVM-Menü) 46
HP BladeSystem Insight Display, Bildschirm „USB Key Menu“ (USB-Schlüssel-Menü) 45
HP BladeSystem Insight Display, Bildschirm „View User Note“ (Benutzernotiz anzeigen) 44
HP BladeSystem Insight Display, Fehlermeldungen
Insight Display-Fehlermeldungen 47
Komponentenausfallfehler 48
Konfigurationsfehler 48
Kühlungsfehler 47
Positionsfehler 48
Stromversorgungsfehler 47
HP BladeSystem Insight Display, Hauptmenü 37
HP BladeSystem Insight Display, Konfigurieren des Gehäuses 31
HP BladeSystem Insight Display, navigieren 37
HP BladeSystem Insight Display, Option „Health Summary“ (Zustand – Zusammenfassung) 39
HP BladeSystem Insight Display, Option „Turn Enclosure UID On/Off“ (Gehäuse-UID aktivieren/deaktivieren) 43
HP BladeSystem Insight Display, zugreifen 30
HP BladeSystem Insight Display-Komponenten
HP BladeSystem c3000 und c7000 3-Zoll Insight Display-Komponenten 29
HP BladeSystem c7000 2-Zoll Insight Display-Komponenten 28
HP Kontaktinformationen 435
HP Partner
HP Kontaktinformationen 435
Support und andere Ressourcen 435

HP Website 435

I
iLO, Prozessorinformationen 253
iLO, Remoteverwaltung 253
iLO-verbundfähig 253
IML (Integrated Management Log) 252
Informationen zum I/O-Erweiterungs-Blade 286
Informationsquellen
HP Kontaktinformationen 435
Verwenden der Online-Hilfe 14
Insight Display
HP BladeSystem Insight Display 28
Insight Display 347
Insight Display – Übersicht 29
Zugreifen auf das HP BladeSystem c3000 Insight Display 30
Insight Display, Bildschirm „KVM Menu“ (KVM-Menü) 46
Insight Display, Bildschirm „USB Key Menu“ (USB-Schlüssel-Menü) 45
Insight Display, navigieren 37
Insight Display, zugreifen 30
Insight Display-Bildschirm, Blade or Port Info (Blade- oder Port-Info) 41
Insight Display-Bildschirm, Chat Mode (Chat-Modus) 44
Insight Display-Bildschirm, Enclosure Info (Gehäuse-Info) 41
Insight Display-Bildschirm, Enclosure Settings (Gehäuseeinstellungen)
Bildschirm „Enclosure Settings“ (Gehäuseeinstellungen) 40
Durchführen der Insight Display-Installation 31
Insight Display-Bildschirm, Health Summary (Zustand – Zusammenfassung) 39
Insight Display-Bildschirm, Turn Enclosure UID On/Off (Gehäuse-UID aktivieren/deaktivieren) 43
Insight Display-Bildschirm, View User Note (Benutzernotiz anzeigen) 44
Insight Display-Fehlermeldungen 47
Insight Display-Komponenten
HP BladeSystem c3000 und c7000 3-Zoll Insight Display-Komponenten 29
HP BladeSystem c7000 2-Zoll Insight Display-Komponenten 28
Insight Remote Support-Registrierung 184
Insight Remote Support-Registrierungsaufhebung 184
Insight Remote Support-Serviceereignisse 192
Installation, Fehler 48
Installieren von DVD-ROM 164
Installieren von Gehäuse-Managementmodulen 25
Installieren von Modulen 25
Installieren von Onboard Administrator-Modulen 25
Integrated Remote Console (IRC) 387
Integration in HP SSO 343
Internetzugriff, aktivieren 136
IP-Adressenzugriff, einschränken 136
IP-Einstellungen, Gehäuse 126
IPv6, aktivieren
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
IPv6 static address (Statische IPv6-Adresse)
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator 212
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
ISO-Abbild
DVD-Laufwerk 162
Enclosure Firmware Management 197
Geräteeinschübe 237

K
Kennwort, streng
FIPS 57
Kennworteinstellungen 327
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140
Kennworteinstellungen 327
Kennwortwiederherstellung, Administrator 15
Komponenten, Beschreibung 3
Komponentenausfall, Fehler 48
Komponentenzusammenfassung 158
Konfiguration, Ändern für Gehäuse und Komponenten 14
Konfigurationsassistent, verwenden
Assistent für die Erstkonfiguration (First Time Setup Wizard) 55
Ausführen des Konfigurationsassistenten 13
Konfigurationsfehler 48
Konfigurationsskripts, verwenden
Konfigurationsskripts 354
Verwenden von Konfigurationsskripts 354
Konfigurationsverwaltung 60
Kontaktaufnahme mit HP
HP Kontaktinformationen 435
Vor der Kontaktaufnahme mit HP 435
Kritische Alarmmeldungen 47

Kryptographische Protokolle
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140
Kühlung, Fehler 47
KVM, Verwendung
Funktionen 50
USB-Registerkarte des aktiven Onboard Administrator-Moduls 211

L

LDAP, Authentifizierung und Zugriffssteuerung
Aktivieren der LDAP-Directory Services-Authentifizierung bei Microsoft Active Directory 390
TFA+LDAP-Authentifizierung 421
Zertifizierungsdienste 390
LDAP+TFA-Authentifizierung 421
LDAP-Authentifizierung, aktivieren
Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 76, 328
LDAP-Gruppe, bearbeiten 339
LDAP-Gruppe, hinzufügen 337
LDAP-Gruppen, verschachtelte
Bildschirm „Directory Groups Configuration“ (Konfiguration von Verzeichnisgruppen) 74
Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 76, 328
Verzeichnisgruppen 335
LDAP-Gruppentest 333
LEDs, Geräteidentifikation (UID) 47
Linux-Unterstützung 350
Location Discovery Services
Anmelden bei der grafischen Benutzeroberfläche von Onboard Administrator 10
Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
Bildschirm „Rack Firmware“ (Rack-Firmware) 106
Bildschirm „Rack Overview“ (Rack-Übersicht) 100
Registerkarte „Rack Topology“ (Rack-Topologie) 103
Lokale Benutzerkonten
Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
Lokale Benutzer 322
lokale Benutzerkonten, aktivieren
Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 76, 328
Lokaler Benutzer, bearbeiten
Edit Local User (Lokalen Benutzer bearbeiten) 323
Lokale Benutzer 322
Lokaler Benutzer, hinzufügen
Add Local User (Lokalen Benutzer hinzufügen) 323
Lokale Benutzer 322
Löschen eines Benutzerkontos
Bildschirm „Local User Accounts“ (Lokale Benutzerkonten) 65
Lokale Benutzer 322
Lüfter, Fehler 47
Lüftermanagement
Management von Lüftern und Kühlung 312
Thermal Subsystem (Thermisches Subsystem) 313
Lüfterstatus 313
Lüftersubsystem, Status 313

M

Management Console, Verbindungsmodule
Bildschirm „Interconnect Bay Summary“ (Zusammenfassung der Verbindungsmoduleinschübe) 286
Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub) 288
Manuelle Aktualisierung
Enclosure Firmware Management 197
Firmware 270
Manuelle Aktualisierung 205
Manuelle Ermittlung 204
Starten einer manuellen Aktualisierung oder Ermittlung 272
Manuelle Ermittlung
Enclosure Firmware Management 197
Firmware 270
Manuelle Ermittlung 204
Starten einer manuellen Aktualisierung oder Ermittlung 272
Mehrere Gehäuse, verwalten 208

N

Navigation 94
Navigation in der grafischen Ansicht 97
Navigation in der Strukturansicht
Änderungen der Strukturansicht und der grafischen Ansicht für HP Integrity i2 Server Blades 357
Strukturansicht 94
Navigieren auf der Benutzeroberfläche 94
Netzredundant, auswählen 296
Netzredundant, Verlust
Power Management 296
Netzteil, Status
Bildschirm „Power Subsystem“ (Stromversorgungs-Subsystem) 310
Netzteilinformationen 311
Netzteile 310
Netzteilredundant, auswählen
Bildschirm „Power Management“ (Stromversorgungsverwaltung) 88
Power Management 296
Netzwerkeinstellungen 79
Netzwerkprobleme 387
Netzwerkzugriff, konfigurieren
Bildschirm „Onboard Administrator Network Settings“ (Onboard

Administrator-Netzwerkeinstellungen) 79
Netzwerkzugriff 136
Registerkarte „Login Banner“ (Anmelde-Banner) 142
NIC Information (NIC-Informationen) 245
NIC settings (NIC-Einstellungen)
Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) 126
Registerkarte „NIC Options“ (NIC-Optionen) 135
Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA 230

O

Onboard Administrator, erstmaliges Ausführen 8
Onboard Administrator, navigieren 94
Onboard Administrator, Redundanz 1
Onboard Administrator, Schnittstellen 6
Onboard Administrator, Übersicht 1
Onboard Administrator-Fehler 360
Onboard Administrator-Modul 25
Onboard Administrator Name 230
Onboard Administrator-Standby-Modul
Bildschirm „Standby Onboard Administrator“ 228
Onboard Administrator Standby-Modul 228
Onboard Administrator-UID, umschalten 229
OpenSSL-Konfigurationsdatei 402
Ozeanien, Zeitzone 432

P

Pinbelegung 352
Planung für das Power Management 295
Polar-Zeit 433
Portzuordnung 255
Portzuordnung, AMC Telco
Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 259
Tabellenansicht der Portzuordnungen der Geräteeinschübe für das c7000-Gehäuse 266
Portzuordnung, grafische Ansicht
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 257
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse 263
Portzuordnung, Server Blade
Änderungen der Portzuordnung für HP Integrity i2 Server Blades 359
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 257
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse 263
Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 259
Portzuordnung, Server Blades doppelter Dichte
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 257
Grafische Ansicht der Portzuordnung der Geräteeinschübe für das c7000-Gehäuse 263
Tabellenansicht der Portzuordnung der Geräteeinschübe für das c3000-Gehäuse 259
Portzuordnung, Verbindungsmoduleinschub 293
Power Management
Bildschirm „Power Management“ (Stromversorgungsverwaltung) 88
Gehäuse-Power Management 295
Power Management 296
Protokolleinschränkungen 136

Q

Quelle der Firmware-Aktualisierung 222

R

Rack-Einstellungen 61
Rack-Übersicht 100
Redundanz 1
Registerkarte CertificateRequest (Zertifikat-Anforderung) 218
Registerkarte CertificateRequest (Zertifikat-Anforderung) des Standby-Moduls 234
Registerkarte CertificateUpload (Zertifikat-Upload) des Standby-Moduls 236
Registerkarte Rack Topology (Rack-Topologie) 103
Registerkarte „Anonymous Data“ (Anonyme Daten) 139
Registerkarte „Firmware Summary“ (Firmware-Zusammenfassung) 270
Registerkarte „IPv4-Einstellungen“
Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
Registerkarte „IPv4 Settings“ (IPv4-Einstellungen)
Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) 126
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen)
Link Loss Failover (Failover bei Verbindungsverlust) 143

Netzwerkzugriff 136
Registerkarte „Advanced Settings“ (Erweiterte Einstellungen) 135
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129
Registerkarte „NIC Options“ (NIC-Optionen) 135
Registerkarte „Language Pack“ (Sprachpaket) des aktiven Onboard Administrator-Moduls 225
Registerkarte „Log Options“ (Protokolloptionen) 227
Registerkarte „NIC Options“ (NIC-Optionen) 135
Registerkarte „Trusted Hosts“ (Vertrauenswürdige Hosts)
Network Access (Netzwerkzugriff) 136
Registerkarte „Trusted Hosts“ (Vertrauenswürdige Hosts) 138
Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des aktiven Onboard Administrator-Moduls 210
Remote Support, Aufheben der Registrierung 184
Remote Support, Datensammlung
Insight Remote Support-Datensammlungen 193
Insight Remote Support-Registrierung 184
Remote Support, Ereignisse 192
Remote Support, Registrierung 184
Remote Support, Voraussetzungen 184
Remote Support, Zertifikatinformationen 194
Remote Support, Zertifikat-Upload/-Download 196
Remote-Systemprotokollierung
Registerkarte „Log Options“ (Protokolloptionen) 227
Systemprotokoll 226
Router Advertisements (Routerankündigungen)
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Registerkarte „IPv6 Settings“ (IPv6-Einstellungen) 129

S

Schnittstellen 6
Secure Boot (Sicherer Systemstart) 245
Serieller Anschluss 352
Server Blade, FRU-Informationen 245
Server Blade, Statusinformationen
Registerkarte mit Informationen zum I/O-Erweiterungs-Blade 286
Registerkarte „Server Blade Information“ (Server Blade-Informationen) 245
Server Blade, virtuelle Geräte 248
Server Blade, Zurücksetzen der Stromversorgung 237
Server Blade-UID, Umschalten 237
Server-Boot-Optionen 250
Servereinschub, Informationen 240
Serverinformationen 245
Service-Port-Verkabelung 353
Sicherer Systemstart, Firmware-Management-Einschränkungen
Enclosure Firmware Management 197
Firmware 270
Geräteeinschübe 237
Registerkarte „Boot Options“ (Startoptionen) 250
Starten einer manuellen Aktualisierung oder Ermittlung 272
Sicherheitschiffren 140
Sicherheitseinstellungen
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140
Sicherheitsprotokolle
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140
Sitzungsoptionen
Konfigurieren des Onboard Administrator-Sitzungszeitlimits 414
Registerkarte „Session Options“ (Sitzungsoptionen) 347
Skriptdateien 60
SNMP-Einstellungen
Bildschirm „Enclosure SNMP Settings“ (SNMP-Gehäuseeinstellungen) 86
SNMP-Einstellungen 143
Sofortzugriff auf DVD 176
Speicher-Blade 279
Sprachpaket 225
SSH, aktivieren 136
SSH Administration (SSH-Verwaltung) 342
SSH-Nachrichtenauthentifizierungscode-Algorithmen 18
SSH-Schlüssel, Austauschalgorithmus 18
SSH-Verschlüsselung 18
SSH-Version, unterstützte 343
SSL-Versionen, unterstützte 343
SSO 343
Standard-Gateway 212
Standby to Active (Standby in Aktiv) 237
Starkes Kennwort
FIPS 57
Registerkarte „FIPS“ 140
Starke Verschlüsselung
FIPS 57
Kryptographische Sicherheitsfunktionen und Standardeinstellungen 18
Registerkarte „FIPS“ 140

Startmodus 245
Startsequenz, Geräteeinschübe 120
Startsequenz, Verbindungseinschübe 123
Status des I/O-Erweiterungs-Blade 284
Statusinformationen, Firmwareaktualisierung 206
Statusinformationen, I/O-Erweiterungs-Blade 284
Statusinformationen, Lüfter 313
Statusinformationen, Netzteil 311
Statusinformationen, Onboard Administrator
Bildschirm „Active Onboard Administrator“ (Aktiver Onboard Administrator) 208
Bildschirm „Standby Onboard Administrator“ 228
Statussymbole 206
Stromobergrenze
Bildschirm „Power and Thermal“ (Stromversorgung und Wärmewerte) 295
Planung für das Power Management 295
Power Management 296
Stromversorgung, Fehler 47
Stromversorgungsredundanz, Verlust
Bildschirm „Power Management“ (Stromversorgungsverwaltung) 88
Power Management 296
Stromverwaltungsoptionen 88
Subnet Mask (Subnetzmaske) 230
Symbole 206
System Log (Systemprotokoll)
Registerkarte „Log Options“ (Protokolloptionen) 227
Systemprotokoll 226
Systemprotokoll
Systemprotokoll für Standby-Onboard Administrator 236
Systemprotokoll, erweitertes 226

T
TCP/IP (Transmission Control Protocol/Internet Protocol) 230
TCP/IP-Einstellungen, über den Standby-Onboard Administrator aufgerufen werden 230
TCP/IP Settings (TCP/IP-Einstellungen)
Bildschirm „Onboard Administrator Network Settings“ (Onboard Administrator-Netzwerkeinstellungen) 79
Bildschirm „TCP/IP Settings“ (TCP/IP-Einstellungen) des aktiven Onboard Administrator 212
Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
Registerkarte „IPv4 Settings“ (IPv4-Einstellungen) 126
Über den aktiven OA angezeigte TCP/IP-Einstellungen für den Standby-OA 230
Technischer Support
HP Kontaktinformationen 435
Support und andere Ressourcen 435
Vor der Kontaktaufnahme mit HP 435
Telefonnummern 435
HP Kontaktinformationen 435
Support und andere Ressourcen 435
Telnet, aktivieren 136
Test-AlertMail 116
Test des Remote-Protokolls 227
Testen, Remote-Protokoll 227
Testen, Verzeichnisservices 333
Testen der Verzeichnisanmeldung 395
TFA+LDAP-Authentifizierung 421
Topologie-Modi 102
Transmission Control Protocol/Internet Protocol (TCP/IP) 230

U
Übersicht 1
Übersicht über die Rack-Firmware 106
UEFI, Startmodus 245
UID-LED 47
Universalzeit, Zeitzone 428
Unterstützung für Gehäuse-iLO-Verbund, aktivieren 136
Unterstützung für iLO-Verbund, Gehäuse 136
USB-Geräte 211
USB-Schlüssel, Unterstützung
DVD-Laufwerk 162
Firmware-Aktualisierung 222
Geräteeinschübe 237

V
Verbinden von Gehäusen 207
Verbindungsausfall, nach dem Neustart
Registerkarte „Trusted Hosts“ (Vertrauenswürdige Hosts) 138
Verschiedene bekannte Probleme 387
Verbindungsmoduleinschub
Bildschirm „Interconnect Bay“ (Verbindungsmoduleinschub) 288
Verbindungsmoduleinschübe 286
Verbindungsmoduleinschub, Management-URL-Informationen 286
Verbindungsmoduleinschub, Menü „UID State“ (UID-Zustand) 286
Verbindungsmoduleinschub, Menü „Virtual Power“ (Virtueller Netzschalter) 286
Verbindungsmoduleinschub, Portzuordnung 293
Verbindungsmoduleinschub, Statusinformationen 291
Verbindungsmoduleinschub, virtuelle Tasten 293
Verbindungsmoduleinschub, Zusammenfassung 286
Verbindungsmoduleinschübe, Startsequenz 123
Verkabelung 25

Verkabelung, Onboard Administrator-Modul 25
Verschlüsselungseinstellungen 18
Vertrauenswürdige IP-Adressen 136
Verwalten der Stromversorgung
  Bildschirm „Enclosure Power Meter“ (Gehäuse-Strommesser) 303
  Power Management 296
Verwalten von Benutzern 320
Verwaltungskonsole, iLO-Remoteverwaltung 253
Verwaltung von Onboard Administrator, Übersicht 4
Verwenden der Online-Hilfe 14
Verzeichnisanmeldung, Testen 395
Verzeichniseinstellungen
  Bildschirm „Directory Settings“ (Verzeichniseinstellungen) 76, 328
  Vorbereiten des Verzeichnisses 390
Verzeichnisgruppe, Einstellungen
  Bearbeiten einer LDAP-Gruppe 339
  Bildschirm „Directory Groups Configuration“ (Konfiguration von Verzeichnisgruppen) 74
  Hinzufügen einer LDAP-Gruppe 337
  Verzeichnisgruppen 335
Verzeichnisgruppe, hinzufügen
  Erstellen von Verzeichnisgruppen 394
  Hinzufügen einer LDAP-Gruppe 337
Verzeichnistest-Einstellungen 333
Verzeichniszertifikat, hochladen 333
Verzeichniszertifikat, Informationen 331
Virtual Connect Manager
  Enclosure TCP/IP Settings (Gehäuse-TCP/IP-Einstellungen) 126
  Registerkarte „IPv4-Einstellungen“ 126
  Virtual Connect Manager 348
Virtuelle Geräte
  DVD-Laufwerk 162
  Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade) 248
Virtuelle Medien, Fehlerbehebung 387
Virtueller Netzschalter 248
Virtuelle Tasten
  Bildschirm „Enclosure Information“ (Gehäuseinformationen) 111
  Registerkarte mit den virtuellen Geräten des I/O-Erweiterungs-Blade 285
  Registerkarte „Server Blade Virtual Devices“ (Virtuelle Geräte des Server Blade) 248
  Registerkarte „Virtual Buttons“ (Virtuellen Tasten) des Onboard Administrator-Standby-Moduls 229
  Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des aktiven Onboard Administrator-Moduls 210
  Virtuelle Tasten des Verbindungsmoduleinschubs 293
Virtuelle Tasten, Gehäuse 111
Virtuelle Tasten, Onboard Administrator
  Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des aktiven Onboard Administrator-Moduls 210
  Registerkarte „Virtual Buttons“ (Virtuelle Tasten) des Onboard Administrator-Standby-Moduls 229
Virtuelle Tasten, Servereinschub 248
Virtuelle Tasten, Verbindungsmoduleinschub 293
VLAN, Konfiguration
  Hinzufügen, Bearbeiten und Entfernen von VLANs 180
  VLAN-Einstellungen 178
  VLAN-Konfiguration 177

W

Warnhinweise 47
Warnmeldungen
  Insight Display-Fehlermeldungen 47
  Komponentenausfallfehler 48
  Konfigurationsfehler 48
  Kühlungsfehler 47
  Positionsfehler 48
  Stromversorgungsfehler 47
Website, HP 435
Werkseinstellungen, zurücksetzen 355

Z

Zertifikat anfordern
  Registerkarte „Certificate Request“ (Zertifikat-Anforderung) 218
  Registerkarte „Certificate Request“ (Zertifikat-Anforderung) des Standby-Moduls 234
Zertifikatsignieranforderung, Antragstellerfeld 423
Zertifikatsignieranforderung, Erstellen
  Erstellen einer Zertifikatsignieranforderung und eines neuen Serverschlüssels 405
  Erstellen von Benutzerschlüsseln und Zertifikatsignieranforderungen 406
Zertifikat-Upload
  Hochladen des DC-Zertifikats (optional) 391
  Hochladen eines Zertifikats 331
  Installieren der Zertifizierungsstellenkette für TFA 415
Zertifikatverwaltung 216

Zertifizierungsdienste, Übersicht
390
ZS (Zertifizierungsstelle),
Installieren für die 2-Faktor-
Authentifizierung 415
Zugreifen auf Onboard
Administrator
Anmelden bei der grafischen
Benutzeroberfläche von
Onboard Administrator 10
Zugriffsanforderungen 3
Zurücksetzen von iLO 237